PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-335273
(43)Date of publication of application : 22.11.2002

(51)Int.Cl. H04L 12/56
H04L 12/46

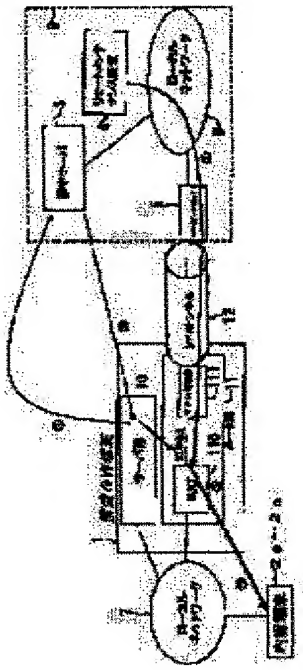
(21)Application number : 2001-350783
(22)Date of filing : 15.11.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NAKAHAMA KIYOSHI
YAMADA KEISHIN

(30)Priority
Priority number : 2001063453 Priority date : 07.03.2001 Priority country : JP

(54) METHOD, SYSTEM AND PROGRAM FOR PERFORMING REMOTE MAINTENANCE AND RECORDING MEDIUM FOR RECORDING THE REMOTE MAINTENANCE PERFORMANCE PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method, program and system for performing remote maintenance capable of remote maintenance on a plurality of Internet gateway terminals and their extension terminals to the utmost at the same time by way of a VPN(Virtual Private Network) on the Internet from a maintenance center while permitting duplicate local network addresses under the control, and to provide a recording medium for recording the remote maintenance execution program.
SOLUTION: The method, program and system for executing remote maintenance adopts a characteristic configuration method realized such that a NAT(network address translation) 110 leading to a local network 7 is provided in a router section 11 in the Internet gateway terminal 1 to convert a global address into a local IP address for VPN NAT thereby allowing the maintenance center 9 to provide/release it.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways, It is a practice which performs remote maintenance from a maintenance center containing the VPN gateway concerned, In a router section in said each Internet gateway terminal, VPNNAT is provided between the local network and VPN treating part, A remote maintenance practice characterized by what said remote maintenance is carried out for by performing grant and release from a maintenance server of said maintenance center by making an address by the side of global into a local IP address for VPNNAT.
[Claim 2]A demand of said remote maintenance in said practice, Said Internet gateway terminal which performs the demand concerned a global IP address of an extension terminal name which is a remote maintenance object, and the Internet gateway terminal concerned, If it notifies to said maintenance server as a remote maintenance demand command, The maintenance server concerned which received the notice concerned a local IP address for VPNNAT and an extension terminal name which are given to said extension terminal for [concerned / which was notified] remote maintenance, Carry out a response to the Internet gateway terminal which has given the notice concerned as a remote maintenance demand response, and. Establishment of a VPN tunnel by IPsec using an authentication key of IPsec shared between global IP addresses of the Internet gateway terminal concerned in the case of a notice of installation is made to set it as a self VPN gateway, Setting out which makes a packet addressed to a local IP address for VPNNAT a VPN processing-object packet of said established VPN tunnel to the VPN gateway concerned is performed, The Internet gateway terminal which received said response acquires a real local IP address to said received extension terminal name, The remote maintenance practice according to claim 1 characterized by a thing which sets a real local IP address to the extension terminal name concerned, and said local IP address for VPNNAT to static NAT, and sets up to a self router section, and for which a series of above processings are carried out one by one.
[Claim 3]As opposed to said extension terminal whose implementation of said remote maintenance is said remote maintenance object, The remote maintenance practice according to claim 2 characterized by what is performed from said maintenance center via said established VPN tunnel by said local IP address for VPNNAT.
[Claim 4]An end of said remote maintenance goes via said established VPN tunnel with said local IP address for VPNNAT first, In a server part which transmitted a remote maintenance quit command, next received the transmission concerned to a server part of said Internet gateway terminal which made the VPN tunnel concerned establish, Perform processing concerning the remote maintenance quit command concerned, and an end response of remote maintenance is transmitted, In then, a maintenance server which received the end response of remote maintenance concerned. The 1st judgment whether all maintenances to an applicable extension terminal were completed is made, In affirmation by the 1st judgment concerned, the ended extension terminal concerned Said server part of said Internet gateway terminal, In denial, a

judging process is ended while making that 2nd judgment which it is in any of said router section, In denial by the 2nd judgment concerned, shift to VPNNAT release processing, and the 3rd judgment whether all remote maintenance to said Internet gateway terminal which corresponds in another side affirmation was ended is made, . While shifting to VPN end processing in affirmation by the 3rd judgment concerned, in denial, end the judging process concerned. The remote maintenance practice according to claim 2 or 3 characterized by what a series of above processings are carried out for one by one.

[Claim 5]Said VPNNAT release processing first a local IP address for VPNNAT to an extension terminal name for [which said maintenance server set up on the occasion of a demand of said remote maintenance / said] remote maintenance, While canceling of a VPN processing-object packet to said established VPN tunnel, After notifying an extension terminal name for [concerned] remote maintenance to said Internet gateway terminal, The Internet gateway terminal which received the notice concerned acquires a real local IP address to the received extension terminal name concerned, The remote maintenance practice according to claim 4 characterized by what a series of above processings in which release static NAT with a local address for VPNNAT to it, and said maintenance server makes said 3rd judgment, and follows the decision result succeedingly are carried out for one by one.

[Claim 6]In said VPN end processing, said maintenance server makes an end of an IPsec session a VPN quit command, The Internet gateway terminal which notified to said Internet gateway terminal and received the notice concerned, An answer to the VPN quit command concerned is transmitted to the maintenance server concerned as an end response of VPN, Said maintenance server makes a demand of said remote maintenance cancel said VPN tunnel set up on the occasion to said VPN gateway, The remote maintenance practice according to claim 4 or 5 characterized by what a series of above processings that end VPN tunnel processing established between the VPN gateway concerned and said Internet gateway terminal are carried out for one by one.

[Claim 7]Said notice of installation by the maintenance server concerned which notified installation notice commands to said maintenance server about the installation concerned, and received the installation notice commands concerned from said server part of said newly installed Internet gateway terminal. An authentication key of IPsec which is the common information for said remote maintenance is generated, Said Internet gateway terminal which carried out the response to said Internet gateway terminal which has notified the installation notice commands concerned, and received the response concerned, The remote maintenance practice according to claim 2, 3, 4, 5, or 6 characterized by a thing which sets up an authentication key of IPsec to said self router section, and for which a series of above processings are carried out one by one.

[Claim 8]In said either one of demand of said remote maintenance or notice of setting out said practice, The remote maintenance practice according to claim 2, 3, 4, 5, 6, or 7 characterized by what VPNNAT setting processing to said server part and said router section of said Internet gateway terminal is carried out for.

[Claim 9]When a failure occurrence is detected to said Internet gateway terminal, said practice, First, the Internet gateway terminal concerned processes information which will start the failure concerned if information which starts failure as a failure information command is transmitted to said maintenance server, next said maintenance server receives said failure information command, It transmits to said Internet gateway terminal which transmitted the failure information command concerned as a failure information response, The remote maintenance practice according to claim 2, 3, 4, 5, 6, 7, or 8 characterized by what a series of above processings in which the Internet gateway terminal concerned which received the failure information response concerned shifts to a demand of said remote maintenance are carried out for one by one.

[Claim 10]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. It is a system which performs remote maintenance from a maintenance

center containing the VPN gateway concerned, NAT is provided between the local network and VPN treating part in a router section in said Internet gateway terminal, A remote maintenance execution system characterized by what is done to functional constitution which performs grant and release from said maintenance center by making an address by the side of global into a local IP address for VPNNAT for a system construction.
[Claim 11]A maintenance server which said maintenance center gives a local address for VPNNAT for VPN access corresponding to an extension terminal name for [concerned] remote maintenance in response to a notice of an extension terminal name for remote maintenance from said Internet gateway terminal, From a remote maintenance device which performs said remote maintenance, and the remote maintenance device concerned. A VPN gateway which goes via access to a local IP address for VPNNAT corresponding to an extension terminal name for [concerned] remote maintenance, The remote maintenance execution system according to claim 10 characterized by what is done for network construction in a maintenance center local network.
[Claim 12]A server part which said Internet gateway terminal notifies that an extension terminal name for remote maintenance is to said maintenance center, By [concerned] having notified. VPNNAT which assigns a local IP address for VPNNAT for VPN access given from the maintenance center concerned, and an IP address of an extension terminal name for [concerned] remote maintenance, and said VPN gateway and a VPN tunnel of the maintenance center concerned. By access to a local IP address for VPNNAT to a remote maintenance object terminal name which consisted of router sections of a VPN treating part to establish, and passed said VPN gateway. The remote maintenance execution system according to claim 10 or 11 characterized by what a function to close packet transfer to said extension terminal from a remote maintenance device which performs said remote maintenance if possible is built for.
[Claim 13]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. . It can set to a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. It is a program used at the Internet gateway terminal concerned, When using remote maintenance service after the Internet gateway terminal concerned is installed, By execution of said program made to carry out to the Internet gateway terminal concerned, notice processing of installation which reports that it installed to said maintenance center. After notifying installation notice commands to a maintenance server of said maintenance center about said installation, A remote maintenance implementation program which sets up an authentication key of IPsec which won popularity as the response concerned when a response to the installation notice commands concerned from the maintenance server concerned was received to a self router section and which is characterized by what a series of above procedures are stepped on for.
[Claim 14]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. . It can set to a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. It is a program used at the Internet gateway terminal concerned, Depending on any of button grabbing by an operator of WEB access from said internal terminal to the Internet gateway terminal concerned, and the Internet gateway terminal concerned they are. By execution of said program made to carry out to the Internet gateway terminal concerned, a remote maintenance request process which requires remote maintenance. After notifying a global IP address of said extension terminal name which is a remote maintenance object, and said Internet gateway terminal to said maintenance server as a remote maintenance demand command, a response to said remote maintenance demand command is received, A real local IP address to an extension terminal name received as the response concerned is acquired, A remote maintenance implementation program to which a real

local IP address to the extension terminal name concerned and a local IP address for VPNNAT received as the response concerned are made to set as static NAT and which is characterized by what a series of above procedures are stepped on for.
[Claim 15]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. . It can set to a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. It is a program used at the Internet gateway terminal concerned, Remote maintenance end processing concerning a notice of a purport that work of said remote maintenance performed from said maintenance center was completed, by execution of said program made to carry out to said inface gateway terminal which received the notice concerned. Ignited by reception of a remote maintenance quit command from said maintenance center, perform processing about the remote maintenance quit command concerned, and an end response of remote maintenance is transmitted, When a notice of an extension terminal name for remote maintenance is received from said maintenance center as a VPN release command, a real local IP address to the received extension terminal name concerned is acquired, A remote maintenance implementation program which releases static NAT with a local address for VPNNAT to an acquired real local IP address and which is characterized by what a series of above procedures are stepped on for.
[Claim 16]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. In a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned, Are a program used in the maintenance center concerned, and a remote maintenance request process corresponding to a demand of said remote maintenance by execution of said program made to perform to said maintenance server. In response to said demand, a local IP address for VPNNAT and an extension terminal name which are given to said extension terminal for [concerning a demand of said remote maintenance] remote maintenance, Transmit to said Internet gateway terminal which performed the demand concerned as a remote maintenance demand response, and. Establishment of a VPN tunnel by IPsec using an authentication key of IPsec shared between global IP addresses of the Internet gateway terminal concerned, Point to a self VPN gateway and the self VPN gateway concerned is received, A remote maintenance implementation program which performs setting out which makes a packet addressed to a local IP address for VPNNAT a VPN processing-object packet of a VPN tunnel established by the directions concerned and which is characterized by what a series of above procedures are stepped on for.
[Claim 17]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. By a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. According to said installation notice commands, setting-out notice-commands processing in which installation notice commands from said Internet gateway terminal which is a program used in the maintenance center concerned, and was newly installed are processed, by execution of said program made to perform to said maintenance center, A remote maintenance implementation program which generates an authentication key of IPsec which is the common information for said remote maintenance, and carries out a response to said Internet gateway terminal which has notified the installation notice commands concerned and which is characterized by what a series of above procedures are stepped on for.
[Claim 18]While carrying out an IP connection to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By

establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. In a system which performs remote maintenance from a single maintenance center containing the VPN gateway concerned, Ignited by being a program used in the maintenance center concerned, and an end button in said maintenance center having been pushed, Remote maintenance end processing which reports that work of said remote maintenance was completed by execution of said program made to perform to said maintenance server. It goes via a VPN tunnel established with a local IP address for VPNNAT, As opposed to a server part of said Internet gateway terminal which made the VPN tunnel concerned establish, If a response of the end of remote maintenance concerned is received after transmitting a remote maintenance quit command, the 1st judgment will be made for that of whether all maintenances to an applicable extension terminal were completed, In affirmation by the 1st judgment concerned, while said ended extension terminal concerned makes that 2nd judgment which it is in any of said server part of said Internet gateway terminal, or a router section, While ending this program in denial and shifting in the 2nd judgment concerned to VPNNAT release processing in denial, The 3rd judgment whether all remote maintenance to said Internet gateway terminal which corresponds in affirmation was ended is made, A remote maintenance implementation program characterized by what a series of above procedures that end this program in denial are stepped on for while shifting to VPN end processing in affirmation by the 3rd judgment concerned.

[Claim 19]Said VPNNAT release processing a local IP address for VPNNAT to an extension terminal name for [which was set up in response to a remote maintenance demand] remote maintenance, Carry out to said VPN gateway and said Internet gateway terminal is received so that it may cancel of a VPN processing-object packet to said established VPN tunnel, After that, notify an extension terminal name for remote maintenance, are a series of processings which carry out a return to said 3rd judgment, and said VPN end processing, It transmits to said Internet gateway terminal by making an end of an IPsec session into a VPN quit command, Said VPN tunnel set up on the occasion of a remote maintenance implementation demand makes said VPN gateway cancel, The remote maintenance implementation program according to claim 18 characterized by a thing which terminates VPN tunnel processing established between the VPN gateway concerned and the Internet gateway terminal concerned, and which they are a series of processings.

[Claim 20]A recording medium which recorded a remote maintenance implementation program characterized by what was done for the nonfiction of a series of procedure by the remote maintenance implementation program according to claim 13, 14, 15, 16, 17, 18, or 19.

[Claim 21]An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet concerned, It is a practice which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned, Before building VPN, said maintenance center which received a VPN construction demand from said Internet gateway terminal chooses a VPN gateway with an empty resource of VPN from two or more VPN gateways of the subordinate dynamically, A global IP address of the selected VPN gateway concerned is notified to the Internet gateway terminal concerned, A remote maintenance practice characterized by what the Internet gateway terminal concerned carries out said remote maintenance for by setting up considering the notified global IP address concerned as an opposite host of the VPN concerned.

[Claim 22]An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet concerned, If it is a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned and a

demand of VPN construction is received from said Internet gateway terminal, A VPN gateway with an empty resource of VPN is dynamically chosen from two or more VPN gateways of the subordinate, Require said VPN construction from said maintenance center which notifies a global IP address of the selected VPN gateway concerned to the Internet gateway terminal which made the demand concerned, and the maintenance center concerned, and. . Provide said said Internet gateway terminal which sets up a global IP address of said notified selected VPN gateway as an opposite host of the VPN concerned from the maintenance center concerned to the demand concerned. A remote maintenance execution system characterized by things.

[Claim 23]An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet concerned, . It can set to a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned. It is a program used at the Internet gateway terminal concerned, Depending on any of registration of a remote maintenance demand from said extension terminal, or button grabbing of said Internet gateway terminal body by the Internet gateway terminal management person they are. By execution of said program made to carry out to the Internet gateway terminal concerned, VPN gateway address request processing in which a VPN gateway address is required. If said VPN gateway address is required from said maintenance center and a VPN gateway address request response to the demand concerned is received from the maintenance center concerned, A VPN gateway global IP address which received as the VPN gateway address request response concerned as an opposite host of VPN, A remote maintenance implementation program which sets it as a self router section and processes said remote maintenance demand and which is characterized by what a series of above procedures are stepped on for.

[Claim 24]An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet, . It can set to a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned. VPN gateway address request processing which is a program used in the maintenance center concerned, and is processing in said maintenance center accompanying a VPN gateway address request from said Internet gateway terminal by execution of said program made to perform to the maintenance center concerned. If said VPN gateway address request is received from said Internet gateway terminal, A VPN gateway with a VPN opening resource is dynamically chosen from two or more VPN gateways under self rule, . Step on a series of above procedures that notify a global IP address of the VPN gateway to the Internet gateway terminal which made the VPN gateway address request concerned. A remote maintenance implementation program characterized by things.

[Claim 25]A recording medium which recorded a remote maintenance implementation program characterized by what was done for the nonfiction of a series of procedure by the remote maintenance implementation program according to claim 23 or 24.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention, VPN is used for extension terminals, such as a personal computer connected to the local network of the Internet gateway terminal itself and its Internet gateway terminal subordinate from the maintenance center connected to the Internet, via the Internet. It is related with the remote maintenance practice which performs remote maintenance, the remote maintenance system directly used for the operation, a program, and the recording medium.
[0002]
[Description of the Prior Art]From the maintenance center conventionally connected to the Internet to the Internet gateway terminal. (Following and ** style GW terminal) The personal computer on the local network connected to the very thing and its ** style GW terminal. There is a method proposed by Japanese Patent Application No. 2000-000496 considering (the following and an extension terminal) as a remote maintenance practice (it is hereafter called VPN remote maintenance) which performs remote maintenance via the Internet using VPN.
[0003]However, in the VPN remote maintenance proposed by the method of Japanese Patent Application No. 2000-000496. When performing remote maintenance simultaneously to two or more ** style GW terminals, When the target ** style GW terminal subordinate's local network address overlaps and a packet is sent to the ** style GW terminal for remote maintenance, and the subordinate's extension terminal via VPN from a maintenance center, In order that an object local IP address may carry out batting, in the VPN gateway by the side of a maintenance center. It was impossible to have performed the maintenance to two or more ** style GW which cannot judge which local net WAKUHE packet I may send out, but have the same local network address simultaneously.
[0004]Then, as a method of maintaining simultaneously to two or more ** style GW which have the same local network address as a subordinate from the inside of the local network of a maintenance center, When the internal network of each ** style GW is seen from the Internet side, the technique with which it is made for the local network address to become unique can be considered.
[0005]The temporary local network address for specifically carrying out VPN communication the maintenance center side inside ** style GW. It is a technique of providing the treating part (following, NATBOX) which fixes and connects (the IP address for the following and VPNNAT), and a local network address, and operation is explained based on drawing 32.
[0006]In drawing 32, in order to show change of the address of a packet in the case of performing IP communication via VPNNAT from client PC (a) to server PC (b), the topology of each node is explained first. It is connected to the private network (c) and client PC (a) has a private IP address of 192.168.2.103. The VPN gateway (d) is connected to the private network (c).
It has 211.0.0.1 as a global IP address by the side of the Internet (e).

[0007]The VPN router (f) is connected to the private network (g).

It has 210.0.0.1 as a global IP address by the side of the Internet.
It is connected to the private network (c) and server PC (b) has a private IP address of 192.168.1.1-192.168.1.254.
[0008]A VPN gateway (d) and ** style GW (it is also hereafter called a VPN router) are building the tunnel (h) of VPN. In the VPN gateway (d), 10.0.0.0/24 is set up as a packet for VPN to the VPN tunnel (h) to a VPN router (b), In the VPN router (b), 192.168.2.0/24 is set up as a packet for VPN to the VPN tunnel (h) of VPN gateway (d) HE.
[0009]NATBOX (f10) has an address of 10.0.0.1-10.0.0.254 in the Internet (e) side as an IP address for VPNNAT, Static NAT is set to 10.0.0.1 by 192.168.1.1, 10.0.0.2, 192.168.1.2, -- (abbreviation),--, 10.0.0.254 and 192.168.1.254.
[0010]If its attention is paid about server PC (b) of 192.168.1.1, here, When the packet of the transmission source address 192.168.1.1 is sent out from the private network (g) side of NATBOX (f10), a transmission source address is rewritten by 10.0.0.1 and sent out to the Internet side of NATBOX (f10), If the packet addressed to transmission destination 10.0.0.1 arrives from the Internet (e) side of NATBOX (f10), a transmission destination address will be rewritten by 192.168.1.1 and will be sent out to the private network (c) side of NATBOX (f10).
[0011]Hereafter, the address change of the packet at the time of communicating between client PC (a) and server PC (b) is shown. Here, the original packet addressed to server PC (b) from client PC (a) is sent out by "a transmitting agency is the 192.168.2.103:transmission destination 10.0.0.1", and reaches a VPN gateway (d).
[0012]Since the VPN gateway (d) received the packet of 10.0.0.1, it judges it as the packet for VPN to the VPN tunnel (h) to a VPN router (f), and it encapsulates by adding the new IP header of "a transmitting agency is the 211.0.0.1:transmission destination 210.0.0.1." It is enciphered and an original packet goes into a data division. This packet reaches the VPN treating part (f11) of a VPN router via a VPN tunnel.
[0013]In the VPN treating part (f11) of a VPN router, an original packet is decrypted and it sends out to NATBOX (f10) as "a transmitting agency is the 192.168.2.103:transmission destination 10.0.0.1." Since static NAT is set up by the outside 10.0.0.1 and the inside 192.168.1.1 and a transmission destination address matches 10.0.0.1 in NATBOX (f10), Address translation is performed, and it becomes "a transmitting agency is the 192.168.2.103:transmission destination 192.168.1.1", and is sent out to the network of a private network (c). Therefore, this packet can reach server PC (b).
[0014]The response original packet from server PC (b) to client PC (a) is sent out by "a transmitting agency is the 192.168.1.1:transmission destination 192.168.2.103", and arrives in the VPN roux evening (f). In a VPN router (f), since 192.168.2.0/24 of packets were received, it is judged as the packet for VPN to the VPN tunnel (h) of VPN gateway (d) HE, and a packet is first sent to NATBOX (f10).
[0015]Since static NAT is set up by the outside 10.0.0.1 and the inside 192.168.1.1 and a transmission source address matches 192.168.1.1 in NATBOX (f10), Address translation is performed, and it becomes "a transmitting agency is the 10.0.0.1:transmission destination 192.168.2.103", and is sent to a VPN treating part (b11).
[0016]a VPN treating part (f11) -- "-- it encapsulates by becoming transmitting agency 210.0.0.1:transmission destination 211.0.0.1", and adding a new IP header. It is enciphered and a response original packet goes into a data division. This packet reaches a VPN gateway (d) via a VPN tunnel (h). In a VPN gateway (d), a response original packet is decrypted, and it becomes "a transmitting agency is the 10.0.0.1:transmission destination 192.168.2.103", and is sent out to the network of a private network (c). Therefore, this packet can reach client PC (a).
[0017]as mentioned above, ** style GW from a maintenance center (f) A static VPNNAT function is applied for the private network (g) of a maintenance center, and the ** style GW (f) subordinate's private network (c) to the case where the number of a subordinate's local networks is one in one set. The operation outline at the time of communicating was explained. The inside of a figure (f1) is a router section which comprises NATBOX (f10) and a VPN treating part (f11).
[0018]The private network (g') (g") of the subordinate of two ** style GW (f') (f") from a

maintenance center Next, those with two, About the case where the private network address overlaps. The operation outline in the case of communicating from the private network (c) of a maintenance center with the application of a static VPNNAT function to each ** style GW (f') (f") subordinate's private network (g') (g") is explained.
[0019]In the case where the private network network address of the subordinate of two ** style GW (f') (f") is the same to drawing 33, How to access simultaneously server PC(b1) - (b4) of two ** style GW (f') (f") subordinates' address from a maintenance center using a static VPNNAT function is shown.
[0020]Here, in order to show change of the address of a packet in the case of performing IP communication via server PC (b1) from client PC (a) - (b4) VPNNAT, the topology of each node is explained first. It is connected to the private network (g') (g"), and client PC (a) has a private IP address of 192.168.2.103. The VPN gateway (d) is connected to the private network (c).
It has 211.0.0.1 as a global IP address by the side of the Internet (e).

[0021]The VPN router (f') is connected to the private network (g').
It has 210.0.0.1 as a global IP address by the side of the Internet (e).
It is connected to the internal local networks 192.168.1.0/24 of a VPN router (f'), and server PC (b1) (b2) has a private IP address of 192.168.1.1-192.168.1.254. The VPN gateway (d) and the VPN router (f') are building the tunnel (h') of VPN.
[0022]In the VPN gateway (d), 10.0.0.0/24 is set up as a packet for VPN to the VPN tunnel (h') to a VPN router (f'), In the VPN router (f'), 192.168.2.0/24 is set up as a packet for VPN to the VPN tunnel (h') of VPN gateway (d) HE.
[0023]NATBOX (f10') has an address of 10.0.0.1-10.0.0.254 in the Internet (e) side as an IP address for VPNNAT, Static NAT is set to 10.0.0.1 by 192.168.1.1, 10.0.0.2, 192.168.1.2, --, (an abbreviation), --, 10.0.0.254 and 192.168.1.254.
[0024]If its attention is paid about server PC (b1) (b2) of 192.168.1.1, here, When the packet of the transmission source address 192.168.1.1 is sent out from the private network (g') side of NATBOX (f10), a transmission source address is rewritten by 10.0.0.1 and sent out to the Internet side of NATBOX (f10'), If the packet addressed to transmission destination 10.0.0.1 arrives from the Internet (e) side of NATBOX (f10'), a transmission destination address will be rewritten by 192.168.1.1 and will be sent out to the private network side of NATBOX (f').
[0025]The VPN router (f") is connected to the private network (g").
It has 210.0.1.1 as a global IP address by the side of the Internet (e).
It is connected to the internal local networks 192.168.1.0/24 of a VPN router (f"), and server PC (b3) (b4) has a private IP address of 192.168.1.1-192.168.1.254.
[0026]The VPN gateway (d) and the VPN router (f") are building the tunnel (h") of VPN. In the VPN gateway (d), 10.0.1.0/24 is set up as a packet for VPN to the VPN tunnel (h") to a VPN router (f"), In the VPN router (f"), 192.168.2 and 0/24 are set up as a packet for VPN to the VPN tunnel (h") of VPN gateway (d) HE.
[0027]NATBOX (f10") has an address of 10.0.1.1-10.0.1.254 in the Internet (e) side as an IP address for VPNNAT, Static NAT is set to 10.0.1.1 by 192.168.1.1, 10.0.1.2, 192.168.1.2, --, (an abbreviation), --, 10.0.1.254 and 192.168.1.254.
[0028]If its attention is paid about server PCB of 192.168.1.1, here, When the packet of the transmission source address 192.168.1.1 is sent out from the private network (g") side of NATBOX (f"), a transmission source address is rewritten by 10.0.1.1 and sent out to the Internet (e) side of NATBOX (f"), If the packet addressed to transmission destination 10.0.1.1 arrives from the Internet (e) side of NATBOX (f"), a transmission destination address will be rewritten by 192.168.1.1 and will be sent out to the private network (g") side of NATBOX (f").
[0029]The private network (g') (g") of the subordinate of two ** style GW (f') (f") from a maintenance center As mentioned above, those with two, About the case where the private network address overlaps. The operation outline in the case of communicating from the private network (c) of a maintenance center with the application of a static VPNNAT function to each ** style GW (f') (f") subordinate's private network (g') (g") was explained.
[0030]Although it is needless to say, operation [said / which was shown / "when those with two

and its private network address overlap in the private network of the subordinate of two ** style GW"], It can apply, "when those with N piece and its private network address overlap in the private network of the subordinate of a ** style GWN (N is arbitrary natural numbers) stand."
[0031]Therefore, by accessing from a maintenance center by the method shown in drawing 33, after building static VPNNAT, When performing remote maintenance simultaneously to two or more ** style GW terminals (VPN router), Even when the target ** style GW terminal subordinate's private network address overlaps, When sending a packet to the ** style GW terminal for remote maintenance, and the subordinate's extension terminal (server PC) via VPN from a maintenance center, By sending out for [by the side of the Internet of NATBOX which assigned the object private IP address by static VPNNAT] addresses, in the VPN gateway by the side of a maintenance center. It can be judged which private net WAKUHE packet I may send out, and it becomes possible to perform the maintenance to two or more ** style GW terminals which have the same private network address simultaneously. Hereafter, this will be called a "static VPNNAT method."
[0032]In the VPN remote maintenance proposed by Japanese Patent Application No. 2000-000496. It made it indispensable for the ** style GW terminal to know the global IP address of the VPN gateway of a maintenance center a priori, and the measure and the method of embedding and shipping the global IP address of a VPN gateway to a ** style GW terminal beforehand were taken.
[0033]
[Problem(s) to be Solved by the Invention]However, when accessing from the private network of a maintenance center to all the private networks of a ** style GW terminal subordinate with said explained "static VPNNAT" method, When building VPN between the ** style GW terminal and the VPN gateway, in the ** style GW terminal, the IP address for VPNNAT and the real local IP address of the private network needed to be assigned by static VPNNAT a priori.
[0034]In this case, it is necessary to assign a priori the IP address resource for VPNNAT (private IP address) which the maintenance center side manages uniquely by the number of a terminal of the private network of the ** style GW terminal subordinate for maintenance. A very huge number of IP address resources for VPNNAT were needed to the number of object terminals which actually maintains. That is, in the static VPNNAT method, when the private IP address of the class was used, only the extension terminal of a maximum of about 16,700,000 sets of ** style GW terminal subordinates was a remote maintenance object terminal.
[0035]For example, the private address of the class is used as an IP address resource for VPNNAT, When all the subnet masks of a ** style GW terminal subordinate's private network are 24 bits and all the subnet masks of a maximum about 65,000 ****** style GW terminal subordinate's private network are 16 bits, only the terminal of the ** style GW terminal subordinate of the maximum about 256 subscription. There were limitations that it could not do with a maintenance object.
[0036]When performing VPN remote maintenance proposed by the method of Japanese Patent Application No. 2000-000496 using a static VPNNAT method, All the extension terminal resources of the ** style GW terminal subordinate who raised the remote maintenance demand had a problem that access will become possible from a maintenance center.
[0037]When the number of the notices of installation of VPN remote maintenance increases and the simultaneous user of VPN remote maintenance service exceeds the number of permission VPN sessions of a VPN gateway, The VPN gateway needed to be extended and installed by the maintenance center side, and a means to make the global IP address of a VPN gateway set it as a terminal in that case did not exist. The method which notifies the Internet gateway administrator of the VPN gateway address of a maintenance center by a certain means and to which a VPN gateway address is made to set manually, Since the help followed on the occasion of remote maintenance, there was a problem of being inapplicable in VPN remote maintenance.
[0038]In here, the main purposes that this invention should be solved are as follows.
[0039]The 1st purpose of this invention is a VPN course of a maintenance center to the Internet, When remote maintenance of two or more ** style GW terminals which permitted duplication of a subordinate's private (local) network address, and its extension terminal is

carried out simultaneously, Restriction of the ** style GW terminal for remote maintenance, and the number of extension terminals, A remote maintenance practice which makes it possible to approve to the maximum of the IP address resource managed by the maintenance center side, and to perform simultaneously remote maintenance of many ** style GW terminals and the subordinate's extension terminal as much as possible, Let a system, a program, and a recording medium be offer plugs.

[0040]The remote maintenance practice, system which do not need to assign a priori the VPNNAT important point IP address resource with which the maintenance center side manages the 2nd purpose of this invention uniquely by the number of a terminal of the private network of the ** style GW terminal subordinate for maintenance, Let a program and a recording medium be offer plugs.

[0041]When performing VPN remote maintenance, the 3rd purpose of this invention, Let the remote maintenance practice, system and program kept access from a maintenance center from taking place to all the extension terminal resources of the ** style GW terminal subordinate who raised the remote maintenance demand, and a recording medium be offer plugs.

[0042]The 4th purpose of this invention needs to extend and install a VPN gateway by the maintenance center side, when the number of the notices of installation of VPN remote maintenance increases and the simultaneous user of VPN remote maintenance exceeds the number of permission VPN sessions of a VPN gateway, but. In that case, let the remote maintenance practice which set the global IP address of the VPN gateway as the terminal, a system, a program, and a recording medium be offer plugs.

[0043]Other purposes of this invention will become naturally clear from the statement of each claim of a specification, a drawing, especially a claim.

[0044]

[Means for Solving the Problem]While carrying out the IP connection of this invention method to an extension terminal of any number by ** each local network and carrying out it the bottom of rule of each Internet gateway terminal in solution of an aforementioned problem, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. It is a practice which performs remote maintenance from a single maintenance center containing the VPN gateway concerned, In a router section in the Internet gateway terminal concerned, VPNNAT is provided between the said local network and VPN treating part, . Carried out by performing grant and release from the maintenance center concerned by making an address by the side of global into a local IP address for VPNNAT. An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to a characteristic configuration method and ** Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet, It is a practice which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned, Before building VPN, said maintenance center which received a VPN construction demand from said Internet gateway terminal chooses a VPN gateway with an empty resource of VPN from two or more VPN gateways of the subordinate dynamically, A global IP address of the selected VPN gateway concerned is notified to the Internet gateway terminal concerned, By setting up considering the notified global IP address concerned as an opposite host of the VPN concerned, the Internet gateway terminal concerned devises a characteristic configuration method which carries out said remote maintenance.

[0045]While carrying out the IP connection of this invention system to an extension terminal of any number by ** each local network and carrying out it the bottom of rule of each Internet gateway terminal in solution of an aforementioned problem, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. It is an execution system which performs remote maintenance from a single maintenance center containing the VPN gateway concerned, In a router section in the Internet gateway terminal concerned, a

VPNNAT means is formed between the said local network and VPN treating part, . Carried out the system construction to functional constitution which can perform grant and release from the maintenance center concerned by making an address by the side of global into a local IP address for VPNNAT. An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to characteristic constituent means and ** Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet, If it is a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned and a demand of VPN construction is received from said Internet gateway terminal, A VPN gateway with an empty resource of VPN is dynamically chosen from two or more VPN gateways of a self subordinate, Require said VPN construction from said maintenance center which notifies a global IP address of the selected VPN gateway concerned to the Internet gateway terminal which made the demand concerned, and the maintenance center concerned, and. A characteristic constituent means which possesses said said Internet gateway terminal which sets up a global IP address of said notified selected VPN gateway as an opposite host of the VPN concerned from the maintenance center concerned to the demand concerned is provided.

[0046]While carrying out the IP connection of this invention program to an extension terminal of any number by ** each local network in solution of an aforementioned problem and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. By a program used in the Internet gateway terminal concerned and the maintenance center concerned by a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. Make an address by the side of global into a local IP address for VPNNAT, and From the maintenance center concerned to grant. An extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself [which was connected to characteristic configuration procedure and ** Internet] which performed various kinds of procedure which releases, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet, By a program used in the Internet gateway terminal concerned and the maintenance center concerned by a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned. The Internet gateway terminal concerned a VPN gateway address which performed a VPNGW address request and was notified from the maintenance server concerned according to the VPNGW address request concerned as an opposite host of VPN, If procedure set as a self router section and the VPNGW address request concerned are received, A VPN gateway with a VPN opening resource is dynamically chosen from two or more VPN gateways under self rule, Characteristic configuration procedure which performed procedure which notifies a global IP address of the VPN gateway to the Internet gateway terminal which made the VPN gateway address request concerned is devised.

[0047]this invention recording medium devises characteristic composition procedure which carried out nonfiction of a series of conclusion procedure by this invention program in solution of an aforementioned problem.

[0048]If it explains in full detail concretely, when this invention devises each new characteristic configuration method, a means, a procedure, or procedure enumerated next, by solution of the technical problem concerned, it will be made as [attain / the above-mentioned purpose].

[0049]While carrying out the IP connection of the 1st feature of this invention method to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways, It is a practice which performs remote maintenance from a maintenance center containing the VPN gateway concerned, In a router

section in said each Internet gateway terminal, VPNNAT is provided between the said local network and VPN treating part, It is in composition adoption of a remote maintenance practice which carries out said remote maintenance by performing grant and release from a maintenance server of said maintenance center by making an address by the side of global into a local IP address for VPNNAT.

[0050]A demand of said remote maintenance in said practice in the 1st feature of an above-mentioned this invention method the 2nd feature of this invention method, Said Internet gateway terminal which performs the demand concerned a global IP address of an extension terminal name which is a remote maintenance object, and the Internet gateway terminal concerned, If it notifies to said maintenance server as a remote maintenance demand command, The maintenance server concerned which received the notice concerned a local IP address for VPNNAT and an extension terminal name which are given to said extension terminal for [concerned / which was notified] remote maintenance, Carry out a response to the Internet gateway terminal which has given the notice concerned as a remote maintenance demand response, and. Establishment of a VPN tunnel by IPsec using an authentication key of IPsec shared between global IP addresses of the Internet gateway terminal concerned in the case of a notice of installation is made to set it as a self VPN gateway, The Internet gateway terminal which performed setting out which makes a packet addressed to a local IP address for VPNNAT a VPN processing-object packet of said established VPN tunnel to the VPN gateway concerned, and received said response, A real local IP address to said received extension terminal name is acquired, It is in composition adoption of a remote maintenance practice which carries out a series of above processings in which set a real local IP address to the extension terminal name concerned, and said local IP address for VPNNAT to static NAT, and it sets up to a self router section, one by one.

[0051]As opposed to said extension terminal whose implementation of said remote maintenance [in / in the 3rd feature of this invention method / the 2nd feature of an above-mentioned this invention method] is said remote maintenance object, It is in composition adoption of a remote maintenance practice which it comes to carry out from said maintenance center via said established VPN tunnel with said local IP address for VPNNAT.

[0052]An end of said remote maintenance [in / in the 4th feature of this invention method / the 2nd or 3rd feature of an above-mentioned this invention method] goes via said established VPN tunnel with said local IP address for VPNNAT first, In a server part which transmitted a remote maintenance quit command, next received the transmission concerned to a server part of said Internet gateway terminal which made the VPN tunnel concerned establish, Perform processing concerning the remote maintenance quit command concerned, and an end response of remote maintenance is transmitted, In then, a maintenance server which received the end response of remote maintenance concerned. The 1st judgment whether all maintenances to an applicable extension terminal were completed is made, In affirmation by the 1st judgment concerned, the ended extension terminal concerned Said server part of said Internet gateway terminal, In denial, a judging process is ended while making that 2nd judgment which it is in any of said router section, In denial by the 2nd judgment concerned, shift to VPNNAT release processing, and the 3rd judgment whether all remote maintenance to said Internet gateway terminal which corresponds in another side affirmation was ended is made, While shifting to VPN end processing in affirmation by the 3rd judgment concerned, it is in composition adoption of a remote maintenance practice which carries out a series of above processings that end the judging process concerned one by one in denial.

[0053]Said VPNNAT release processing in the 4th feature of an above-mentioned this invention method the 5th feature of this invention method, First, a local IP address for VPNNAT to an extension terminal name for [which said maintenance server set up on the occasion of a demand of said remote maintenance / said] remote maintenance, While canceling of a VPN processing-object packet to said established VPN tunnel, After notifying an extension terminal name for [concerned] remote maintenance to said Internet gateway terminal, The Internet gateway terminal which received the notice concerned acquires a real local IP address to the received extension terminal name concerned, Static NAT with a local address for VPNNAT to it

is released, and it is in composition adoption of a remote maintenance practice in which said maintenance server carries out a series of above processings in which make said 3rd judgment and the decision result is followed, one by one succeedingly.
[0054]In said VPN end processing [in / in the 6th feature of this invention method / the 4th or 5th feature of an above-mentioned this invention method], said maintenance server makes an end of an IPsec session a VPN quit command, The Internet gateway terminal which notified to said Internet gateway terminal and received the notice concerned, An answer to the VPN quit command concerned is transmitted to the maintenance server concerned as an end response of VPN, Said maintenance server makes a demand of said remote maintenance cancel said VPN tunnel set up on the occasion to said VPN gateway, It is in composition adoption of a remote maintenance practice which carries out a series of above processings that end VPN tunnel processing established between the VPN gateway concerned and said Internet gateway terminal one by one.
[0055]Said notice of installation in the 2nd, 3rd, 4th, 5th, or 6th feature of an above-mentioned this invention method the 7th feature of this invention method, By the maintenance server concerned which notified installation notice commands to said maintenance server about the installation concerned, and received the installation notice commands concerned from said server part of said newly installed Internet gateway terminal. An authentication key of IPsec which is the common information for said remote maintenance is generated, Said Internet gateway terminal which carried out the response to said Internet gateway terminal which has notified the installation notice commands concerned, and received the response concerned, It is in composition adoption of a remote maintenance practice which carries out a series of above processings in which an authentication key of IPsec is set up to said self router section, one by one.
[0056]In said either one of demand of said remote maintenance or notice of setting out said practice in the 2nd, 3rd, 4th, 5th, 6th, or 7th feature of an above-mentioned this invention method the 8th feature of this invention method, It is in composition adoption of a remote maintenance practice which carries out VPNNAT setting processing to said server part and said router section of said Internet gateway terminal.
[0057]Said practice in the 2nd, 3rd, 4th, 5th, 6th, 7th, or 8th feature of an above-mentioned this invention method the 9th feature of this invention method, When a failure occurrence is detected to said Internet gateway terminal, First, the Internet gateway terminal concerned processes information which will start the failure concerned if information which starts failure as a failure information command is transmitted to said maintenance server, next said maintenance server receives said failure information command, It transmits to said Internet gateway terminal which transmitted the failure information command concerned as a failure information response, The Internet gateway terminal concerned which received the failure information response concerned is in composition adoption of a remote maintenance practice which carries out a series of above processings that shift to a demand of said remote maintenance one by one.
[0058]The 10th feature of this invention method an extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet concerned, It is a practice which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned, Before building VPN, said maintenance center which received a VPN construction demand from said Internet gateway terminal chooses a VPN gateway with an empty resource of VPN from two or more VPN gateways of the subordinate dynamically, A global IP address of the selected VPN gateway concerned is notified to the Internet gateway terminal concerned, By setting up considering the notified global IP address concerned as an opposite host of the VPN concerned, the Internet gateway terminal concerned is in composition adoption of a remote maintenance practice which carries out said remote maintenance. (It corresponds to claim 21)
[0059]While carrying out the IP connection of the 1st feature of this invention system to an

extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. It is a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned, NAT is provided between the local network and VPN treating part in a router section in said Internet gateway terminal, It is in composition adoption of a remote maintenance execution system which carries out a system construction to functional constitution which performs grant and release from said maintenance center by making an address by the side of global into a local IP address for VPNNAT.

[0060]Said maintenance center in the 1st feature of the above-mentioned this invention system the 2nd feature of this invention system, A maintenance server which gives a local address for VPNNAT for VPN access corresponding to an extension terminal name for [concerned] remote maintenance in response to a notice of an extension terminal name for remote maintenance from said Internet gateway terminal, From a remote maintenance device which performs said remote maintenance, and the remote maintenance device concerned. It is in composition adoption of a remote maintenance execution system which carries out network construction of the VPN gateway which goes via access to a local IP address for VPNNAT corresponding to an extension terminal name for [concerned] remote maintenance in a maintenance center local network.

[0061]A server part for which said Internet gateway terminal [in / in the 3rd feature of this invention system / the 1st or 2nd feature of the above-mentioned this invention system] notifies an extension terminal name for remote maintenance to said maintenance center, By [concerned] having notified. VPNNAT which assigns a local IP address for VPNNAT for VPN access given from the maintenance center concerned, and an IP address of an extension terminal name for [concerned] remote maintenance, and said VPN gateway and a VPN tunnel of the maintenance center concerned. By access to a local IP address for VPNNAT to a remote maintenance object terminal name which consisted of router sections of a VPN treating part to establish, and passed said VPN gateway. It is in composition adoption of a remote maintenance execution system which builds a function to close packet transfer to said extension terminal from a remote maintenance device which performs said remote maintenance if possible.

[0062]The 4th feature of this invention system an extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet concerned, If it is a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned and a demand of VPN construction is received from said Internet gateway terminal, A VPN gateway with an empty resource of VPN is dynamically chosen from two or more VPN gateways of the subordinate, Require said VPN construction from said maintenance center which notifies a global IP address of the selected VPN gateway concerned to the Internet gateway terminal which made the demand concerned, and the maintenance center concerned, and. A global IP address of said selected VPN gateway notified [aforementioned] from the maintenance center concerned to the demand concerned, It is in composition adoption of a remote maintenance execution system possessing said Internet gateway terminal set up as an opposite host of the VPN concerned. (It corresponds to claim 22)

[0063]While carrying out the IP connection of the 1st feature of this invention program to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. . It can set to a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. It is a program used at the Internet gateway terminal concerned, When using remote maintenance service after the Internet gateway terminal concerned is installed, By execution of said program made to carry out to the Internet gateway terminal concerned, notice processing of installation which reports

that it installed to said maintenance center. . After notifying installation notice commands to a maintenance server of said maintenance center about said installation, set up an authentication key of IPsec which won popularity as the response concerned when a response to the installation notice commands concerned from the maintenance server concerned was received to a self router section. It is in composition adoption of a remote maintenance implementation program which steps on a series of procedures.

[0064]While carrying out the IP connection of the 2nd feature of this invention program to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. . It can set to a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. It is a program used at the Internet gateway terminal concerned, Depending on any of button grabbing by an operator of WEB access from said internal terminal to the Internet gateway terminal concerned, and the Internet gateway terminal concerned they are. By execution of said program made to carry out to the Internet gateway terminal concerned, a remote maintenance request process which requires remote maintenance. After notifying a global IP address of said extension terminal name which is a remote maintenance object, and said Internet gateway terminal to said maintenance server as a remote maintenance demand command, In response to a response to said remote maintenance demand command, a real local IP address to an extension terminal name received as the response concerned is acquired, It is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures to which a real local IP address to the extension terminal name concerned and a local IP address for VPNNAT received as the response concerned are made to set as static NAT.

[0065]While carrying out the IP connection of the 3rd feature of this invention program to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. . It can set to a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. It is a program used at the Internet gateway terminal concerned, Remote maintenance end processing concerning a notice of a purport that work of said remote maintenance performed from said maintenance center was completed, by execution of said program made to carry out to said inface gateway terminal which received the notice concerned. Ignited by reception of a remote maintenance quit command from said maintenance center, perform processing about the remote maintenance quit command concerned, and an end response of remote maintenance is transmitted, When a notice of an extension terminal name for remote maintenance is received from said maintenance center as a VPN release command, A real local IP address to the received extension terminal name concerned is acquired, and it is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures of releasing static NAT with a local address for VPNNAT to an acquired real local IP address.

[0066]While carrying out the IP connection of the 4th feature of this invention program to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. In a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned, Are a program used in the maintenance center concerned, and a remote maintenance request process corresponding to a demand of said remote maintenance by execution of said program made to perform to said maintenance server. In response to said demand, a local IP address for VPNNAT and an extension terminal name which are given to said extension terminal for [concerning a demand of said remote maintenance] remote maintenance, Transmit to said Internet gateway terminal which performed the demand concerned as a remote maintenance demand response, and. Establishment of a VPN tunnel by IPsec using an authentication key of IPsec shared

between global IP addresses of the Internet gateway terminal concerned. Point to a self VPN gateway and the self VPN gateway concerned is received, It is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures of performing setting out which makes a packet addressed to a local IP address for VPNNAT a VPN processing-object packet of a VPN tunnel established by the directions concerned.
[0067]While carrying out the IP connection of the 5th feature of this invention program to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. By a system which performs remote maintenance from a maintenance center containing the VPN gateway concerned. According to said installation notice commands, setting-out notice-commands processing in which installation notice commands from said Internet gateway terminal which is a program used in the maintenance center concerned, and was newly installed are processed, by execution of said program made to perform to said maintenance center, It is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures that generate an authentication key of IPsec which is the common information for said remote maintenance, and carry out a response to said Internet gateway terminal which has notified the installation notice commands concerned.
[0068]While carrying out the IP connection of the 6th feature of this invention program to an extension terminal of any number by each local network and carrying out the bottom of rule of each Internet gateway terminal, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model via each Internet gateway terminal concerned and Internet between VPN gateways. In a system which performs remote maintenance from a single maintenance center containing the VPN gateway concerned, Ignited by being a program used in the maintenance center concerned, and an end button in said maintenance center having been pushed, Remote maintenance end processing which reports that work of said remote maintenance was completed by execution of said program made to perform to said maintenance server. It goes via a VPN tunnel established with a local IP address for VPNNAT, As opposed to a server part of said Internet gateway terminal which made the VPN tunnel concerned establish, If a response of the end of remote maintenance concerned is received after transmitting a remote maintenance quit command, the 1st judgment will be made for that of whether all maintenances to an applicable extension terminal were completed, In affirmation by the 1st judgment concerned, while said ended extension terminal concerned makes that 2nd judgment which it is in any of said server part of said Internet gateway terminal, or a router section, While ending this program in denial and shifting in the 2nd judgment concerned to VPNNAT release processing in denial, The 3rd judgment whether all remote maintenance to said Internet gateway terminal which corresponds in affirmation was ended is made, While shifting to VPN end processing in affirmation by the 3rd judgment concerned, it is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures that end this program in denial.
[0069]Said VPNNAT release processing in the 6th feature of the above-mentioned this invention program the 7th feature of this invention program, A local IP address for VPNNAT to an extension terminal name for [which was set up in response to a remote maintenance demand] remote maintenance, Carry out to said VPN gateway and said Internet gateway terminal is received so that it may cancel of a VPN processing-object packet to said established VPN tunnel, Notify an extension terminal name for remote maintenance, and after that, are a series of processings which carry out a return to said 3rd judgment, and said VPN end processing makes an end of an IPsec session a VPN quit command, Transmit to said Internet gateway terminal and to said VPN gateway. Said VPN tunnel set up on the occasion of a remote maintenance implementation demand makes it cancel, and it is in composition adoption of a remote maintenance implementation program which are a series of processings in which VPN tunnel processing established between the VPN gateway concerned and the Internet gateway terminal concerned is terminated.

[0070]The 8th feature of this invention program an extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet concerned, . It can set to a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned. It is a program used at the Internet gateway terminal concerned, Depending on any of registration of a remote maintenance demand from said extension terminal, or button grabbing of said Internet gateway terminal body by the Internet gateway terminal management person they are. By execution of said program made to carry out to the Internet gateway terminal concerned, VPN gateway address request processing in which a VPN gateway address is required. If said VPN gateway address is required from said maintenance center and a VPN gateway address request response to the demand concerned is received from the maintenance center concerned, A VPN gateway global IP address which received as the VPN gateway address request response concerned as an opposite host of VPN, It is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures of setting it as a self router section and processing said remote maintenance demand. (It corresponds to claim 23)
[0071]The 9th feature of this invention program an extension terminal by which the IP connection was carried out to a local network of two or more Internet gateway terminal itself connected to the Internet, and a subordinate of those, By establishing IPsec which realizes a VPN session in a network layer of open systems interconnection reference model between VPN gateways connected to the Internet gateway terminal concerned and the Internet, . It can set to a system which performs remote maintenance from a single maintenance server of the VPN gateway subordinate concerned. VPN gateway address request processing which is a program used in the maintenance center concerned, and is processing in said maintenance center accompanying a VPN gateway address request from said Internet gateway terminal by execution of said program made to perform to the maintenance center concerned. If said VPN gateway address request is received from said Internet gateway terminal, . Choose a VPN gateway with a VPN opening resource from two or more VPN gateways under self rule dynamically, and notify a global IP address of the VPN gateway to the Internet gateway terminal which made the VPN gateway address request concerned. It is in composition adoption of a remote maintenance implementation program which steps on a series of above procedures. (It corresponds to claim 24)
[0072]The 1st feature of this invention recording medium is in composition adoption of a recording medium which recorded a remote maintenance implementation program which carries out nonfiction of a series of procedure by said program in the 1st, 2nd, 3rd, 4th, 5th, 6th, or 7th feature of the above-mentioned this invention program.
[0073]The 2nd feature of this invention recording medium is in composition adoption of a recording medium which recorded a remote maintenance implementation program which carries out nonfiction of a series of procedure by said program in the 7th or 9th feature of the above-mentioned this invention program. (It corresponds to claim 25)
[0074]
[Embodiment of the Invention]Hereafter, with reference to an accompanying drawing, details are explained for an embodiment of the invention about the example of a system, the example of a method, the example of a recording medium, and an example program.
[0075](Example of a system) The lineblock diagram of the example of a remote maintenance execution system which is one embodiment of this invention is shown in drawing 1. The system construction of the remote maintenance system is carried out from the Internet gateway terminal 1 (following and ** style GW terminal), the extension terminals 2a-2n (n expresses arbitrary natural numbers), the maintenance server 3, the remote maintenance device 4, and five nodes of VPN gateway 5 (5a-5n).
[0076]Said ** style GW terminal 1 is premised on usually communicating with all by the side of extension (LAN) seven which is a local network, by TCP/IP the Internet 6 (WAN) side. Necessity

has had a function in which VPN gateway 5 (5a-5n) and VPN on LAN8 by the side of the maintenance server 3 can be built.
[0077]The thing called the conventional router f and an application gateway is applicable. Like the conventional ISDN evening-MINARU adapter, the thing which does not communicate TCP/IP is not made into an object by itself. In the following description, the name of a "terminal" only points out the ** style GW terminal 1.
[0078]Said extension terminals 2a-2n are terminals (group) of PC (personal computer) linked to extension LAN7 of said ** style GW terminal 1 subordinate, etc. The server part 10 and the router section 11 which are contained in ** style GW terminal 1 main part connected to extension LAN7 are also treated as the extension terminals 2a-2n. Said maintenance center 9 is a general term for the center which performs remote maintenance which makes a component the maintenance server 3, the remote maintenance device 4, and VPN gateway 5 (5a-5n).
[0079]Said maintenance server 3 is a server on the Internet 6 which manages the information about the ** style GW terminal 1 and extension terminals [2a-2n] remote maintenance, and has a LAN interface in the LAN8 side in which the remote maintenance device 4 exists respectively the Internet 6 side.
[0080]Said remote maintenance device 4 is an operating device which performs the ** style GW terminal 1 and extension terminals [2a-2n] remote maintenance, and it is a premise to have a WEB browser function. Said VPN gateways 5a-5n are Internet 6 courses, and are the VPN gateway devices for building VPN which connects the maintenance center 9 to the ** style GW terminal 1.
[0081]The http server part 100 in which said ** style GW terminal 1 performs http server processing, The CGI treating part 101 which is called from a http server and performs internal processing, It comprises the router setting processing part 102 which publishes the control commands to the router section 11, the server part 10 containing the command sending-out treating part 103 which transmits a command to the maintenance server 3, and the router section 11 which controls the IP router processing having contained IPsec.
[0082]Said maintenance server 3 comprises the http server part 30 which receives the http command from the terminal 1, the CGI treating part 31 which is called from the http server part 30 and performs internal processing, and the VPN gateway setting processing part 32 which publishes a VPN gateway 1 HE telnet command. Said VPN gateways 5a-5n comprise the router section 11 of the terminal 1, the VPN treating part 50 which performs a VPN session, and the setting command receiving processing part 51 which receives the telnet command from the maintenance server 3.
[0083]Said remote maintenance device 4 comprises the maintenance command processing part 40 which sends out a command to the server part 10 of the terminal 1 with a http protocol etc. As mentioned above, using the shown maintenance server 3, VPN gateways 5a-5n, and the remote maintenance device 4 by the VPN tunnel 12 course of the Internet 6 from the maintenance center 9. When carrying out remote maintenance of two or more ** style GW terminals 1 and its extension terminals 2a-2n, ** style GW terminal 1 subordinate's local network address realizes VPN remote maintenance simultaneously by any cases.
[0084](Example of a method) The VPN remote maintenance in this example of a method applied to said example of a system, The notice processing of installation, a VPNGW address request, and a remote maintenance request process, Remote maintenance end processing, VPNNAT release processing, and VPN end processing, "Remote maintenance implementation" (in this remote maintenance protocol, the protocol in particular of actual maintenance work is not specified.) which the operator of the maintenance center 9 actually performs with seven "notice commands and responses" with failure information processing As long as it uses TCP/IP, it may be general-purpose application and an original protocol may be sufficient as it. It is constituted as a communications protocol.
[0085]Seven communications protocols other than remote maintenance implementation are only the techniques for performing actual maintenance work (henceforth, remote maintenance implementation) here, and the main point is as follows to the last.
[0086]From the remote maintenance device 4, to the maintenance object extension terminals

2a-2n, perform the first main point and with the application which uses a TCP/IP protocol using the tunnel 12 of VPN At namely, this time. The local IP address for VPNNAT is used for the IP connection from the remote maintenance device 4 of the maintenance center 9 to the maintenance object extension terminals 2a-2n, It is in carrying out certainly access to two or more ** style GW terminals 1 described previously, even when the subordinate's IP address overlaps by carrying out by after-mentioned VPNNAT110 which carries out functional constitution into the router section 11. However, if it goes via the NAT concerned, limitations cannot carry out application which cannot be carried out.

[0087]From the remote maintenance device 4, to the maintenance object extension terminals 2a-2n, perform the 2nd main point and with the application which uses a TCP/IP protocol using the tunnel 12 of VPN At this time. Even when an address is changed by extension etc., VPN gateways 5a-5n of the maintenance center 9 via arbitrary VPN gateways 5a-5n and the Internet gateway from the remote maintenance device 4, It is in the IP connection to a maintenance object extension terminal being performed certainly.

[0088]Hereafter, this example of a method for attaining said first main point is explained with reference to drawings below. There is this example of a method concerned in giving the local IP address for VPNNAT dynamically to VPNNAT110 which carries out functional constitution into the router section 11. The outline of the function which gives the local IP address for VPNNAT dynamically to VPNNAT110 based on drawing 2 is explained.

[0089]First, the extension terminal 2a-2n person of a remote maintenance object terminal is notified to the maintenance center 9 by **. ** The maintenance center 9 gives the local IP address (10.0.0.1) for VPNNAT for VPN access corresponding to the extension terminal 2a-2n person for remote maintenance by the server part 10 course of the ** style GW terminal 1 to the ** style GW terminal 1. This is fundamentally performed at the time of a remote maintenance demand.

[0090]Next, by **, the local IP address for VPNNAT and an extension terminals [for remote maintenance / 2a-2n] IP address are assigned static NAT110. This is also performed to a remote maintenance demand following on **. Next, local IP address hair KUSESU for VPNNAT is carried out [be / it / under / of VPN tunnel 12 / letting it pass] by ** at the time of remote maintenance implementation. If it does so, as shown in **, extension terminal 2a-2n HEPAKETTO for remote maintenance will be transmitted, and it will become accessible.

[0091]Thus, by giving the local IP address for VPNNAT dynamically, even if it does not assign the local IP address for VPNNAT statically a priori, Access to two or more ** style GW terminals 1 can be simultaneously considered as operation, even when the subordinate's IP address overlaps.

[0092]In advance of VPN construction, the maintenance center 9 chooses dynamically VPN gateway 5i with the resource of the empty of VPN from two or more VPN gateways 5a-5n of the subordinate hereafter as an example of a method which attains the 2nd main point, It is in carrying out setting-out grant of the global IP address of the VPN gateway installed in the router section 11 as an opposite host of VPN dynamically by notifying to the router section 11 of a ** style GW terminal.

[0093]Hereafter, an outline is explained about six protocols for realizing this example of a method. Said notice processing of installation notifies the maintenance server 3 that the ** style GW terminal 1 was installed, It is main point to encipher and receive the common informations (Preshared Key of IPsec, a terminal authentication password (following, Secret (ID2)), etc.) for remote maintenance from the maintenance server 3.

[0094]In order to realize said main point, it is also the big purpose also within the notice processing of installation to build VPNNAT110 to the server part 10 and the router section 11 of the ** style GW terminal 1 in this example of a method.

[0095]Said VPNGW address request processing chooses dynamically VPN gateway 5i with the resource of the opening of VPN from VPN gateways 5a-5n of maintenance center 9 subordinate's plurality [server / 3 / maintenance], It notifies to the ** style GW terminal 1 by making the global IP address of the VPN gateway 5i into the notice response of a VPN gateway, It is also big main point in this method that the ** style GW terminal router section 11 sets up

considering the global IP address of notified VPN gateway 5i as an opposite host of VPN.
[0096]Said remote maintenance request process makes it main point to require implementation of the remote maintenance by IPsec of the maintenance server 3. Let the maintenance object terminals corresponding to a remote maintenance request process be ** style GW terminal 1 main part and the extension terminals 2a-2n. In order to realize main point, in this example of a method, big main point also builds VPNNAT110 also within a remote maintenance request process to the server part 10 of the ** style GW terminal 1, and extension terminals 2a-2n other than router section 11.
[0097]Said remote maintenance end processing makes it main point to tell that remote maintenance was actually completed using the remote maintenance device 4 to the target ** style GW terminal 1.
[0098]Said VPNNAT110 release processing is aimed at releasing VPNNAT110 about the server part 10 of the ** style GW terminal 1 which remote maintenance ended, and extension terminals 2a-2n other than router section 11. Thereby, effective use of the local IP address resources for VPNNAT is attained so that it may state to a next effect. VPN end processing makes it main point to end an IPsec session.
[0099](An example program, the example of a recording medium) The example program and the example of a recording medium for carrying out this example of a method are explained per drawing. The flow of each commo data is shown using whole remote maintenance process flow drawing 3 - drawing 9. "->" of each figure The notice processing of installation, VPNGW address request processing, a remote Menten Nance request process, It is the procedure and the flow of procedure which showed command sending out and reception in a communication sequence of remote maintenance end processing, VPNNAT release processing, VPN end processing, and failure information processing in the case.
[0100]Processing carries out an opportunity [operation of ** style GW terminal 1 installer] only once at the time of ** style GW terminal 1 installation, ** installation notice commands (terminal ID and a public key.) of the notice processing of installation shown in drawing 3The original text, the notice response of MAC->** installation (and) [encryption] Encryption Secret ID2, an encryption maintenance-man password, the local IP address for VPNNAT for encryption server parts, The local IP address for VPNNAT for encryption router sections and local IP address ->** router setting out for VPNNAT for encryption router sections (VPNNAT110, encryption Preshared Key) are performed.
[0101]Then, an extension terminal 2a-2n user (the following, user) receives the maintenance center 9 (the following, center) from the ** style GW terminal 1, When extension terminals [2a-2n] remote maintenance was required, whenever it planned, every, it carries out an opportunity [an extension terminal user's operation], **VPNGW address request command (terminal ID.) of the VPNGW address request shown in drawing 4Public key, original text, and MAC->**VPNGW selection process ->**VPNGW address request response (VPN gateway global IP address) ->** router setting out (VPN gateway global IP address) is performed.
[0102]next, ** remote maintenance demand command (terminal ID.) of the remote maintenance demand shown in drawing 5 ignited by the end of processing of a VPNGW address request Extension terminal 2a-2n a person and a ** style GW terminal global address, a claimant level, urgency, a claimant name, a telephone number, and the routing configuration ->**IPsec setting processing ->** remote maintenance demand response for the local IP addresses for local IP address quota processing ->**VPNNAT for request content ->**VPNNAT (an extension terminal 2a-2n person.) VPNNAT110 setting out of the local IP address for VPNNAT and the local IP address for number-of-acceptance ->**VPNNAT is performed.
[0103]In the center 9, the operator is checking reception of a remote maintenance demand at any time from the remote maintenance device 4. When the operator carried out remote maintenance to each remote maintenance request process, whenever it planned, ** remote maintenance implementation shown in drawing 6 is performed by operation of an operator every.
[0104]In the center 9, whenever the remote maintenance to each remote maintenance request process was completed, every by operation of an operator. ** remote maintenance quit command of remote maintenance end processing shown in drawing 7 (number of acceptance) ->

the end response of ** remote maintenance is performed.
[0105]By judgment of the maintenance server 3 after remote maintenance end processing if needed. Automatically, To drawing 8. The **VPNNAT110 release command of the shown VPNNAT release processing. (Extension terminal 2a-2n person) local IP address VPNNAT reset ->**VPNNAT110 release response for ->**VPNNAT -> -- the object for **VPNNAT -- local -- local IP address routing configuration release for IP address translation processing ->**VPNNAT is performed.
[0106]By judgment of the maintenance server 3 after the end of VPNNAT110 release if needed. The routing initialization ->**IPsec reset for end response ->**VPNNAT of local IP address initialization setting-out ->**VPN of the end of VPN automatically shown in drawing 9 for local IP addresses for **VPN quit-command ->**VPNNAT is performed.
[0107]The above is an outline of a whole flow. The process flow of the ** style GW terminal 1 at the time of paying one's attention to one ** style GW terminal and the maintenance center 9 is shown in the flow chart of drawing 10 and drawing 11.
[0108]Namely, about the ** style GW terminal 1 side flow chart shown in drawing 10. The notice STc of installation steps on STa->STb one by one, and is practiced, and the remote maintenance end processing STh steps on STd->STe from the notice STc of installation, The VPNNAT release processing STi steps on STd->STe->STf from the notice STc of installation, The VPN end processing STj steps on STd->STe->STf->STg from the notice STc of installation, The failure information STn steps on STd->STk->STl from the notice STc of installation, The VPNGW address request STo steps on STd->STk from the notice STc of installation, or from the failure information STn, link directly and it steps on it, The remote maintenance demand STm steps on STd->STk->STo from the notice STc of installation, or steps on STd->STk->STl->STn->STo, it practices, respectively, and a repetition enters in the meantime if needed.
[0109]About the center 9 side flow chart (** style GWID=N) shown in drawing 11. VPNGW address request processing ST16 ST1 ->ST2 ->ST3 notice processing STof installation 6 ST1 ->ST2 ->ST3 ->ST15, Remote maintenance request process ST7 steps on ST1 ->ST2 ->ST3 ->ST15 ->ST4, failure information processing ST8 steps on ST1 ->ST2 ->ST3 ->ST15 ->ST4 ->ST5 one by one, respectively, and it practices.
[0110]End STof remote maintenance 9 steps on ST1 ->ST2, and VPNNAT release ST12 steps on end STof remote maintenance 9 to ST10 ->ST11, End STof VPN 14 steps on VPNNAT release ST12 to ST13, it practices, respectively, and a repetition enters in the meantime if needed. Although notified at the time of a failure occurrence, since it is processing independent of the whole flow, it does not touch with the failure information shown in drawing 26 in detail here.
[0111][Precondition for remote maintenance implementation] In addition, in order to perform this example of an embodiment, the following preconditions are required.
(1) Share ******** information (following, Secret (ID)) between the maintenance server 3 and the terminal 1 a priori. Secret (ID) is embedded at ROM etc. at the terminal 1 at the time of shipment, and corresponds by sharing with the maintenance server 3. Secret (ID) presupposes that it is common to all the terminals 1 in which the maintenance server 3 performs a remote maintenance.
[0112](2) The router section 11 of the terminal 1 should have a VPN function of IP levels, such as IPsec. What setting out by the side of the waiting receptacle for a session is performed for a priori about the VPN session (in the case of IPsec, it sets up as responder). What Preshared key sets up dummy data for.
(3) VPN gateway 5 of the maintenance center 9 performs setting out by the side of session setup a priori about a VPN session (in the case of IPsec, it sets up as an initiator).
[0113](4) VPN gateway 5 should have a VPN function with the router section 11 of the terminal 1, and communication compatibility.
(5) Know the router section 11 of the terminal 1 a priori by the point in time of the notice of installation of the global IP address (or Internet host name) to which the maintenance server 3 was opened. The Internet 6 HE connections set should be completed.

[0114](6) Perform various setting out to the router section 11 from the router setting processing part 102 by a remote console (following, telnet) or interprocess communication (socket communication etc.).
(7) Perform various setting out to the setting command receiving processing part 51 of VPN gateway 5 from the VPN gateway setting processing part 32 of the maintenance server 3 by telnet or interprocess communication (socket communication etc.).
[0115](8) On the maintenance server 3, it has VPNNAT110DB. A table comprises two or more records which used the local IP address for VPNNAT as the key, is assigned as the field, and has ** style GW terminal ID / terminal name.
(9) It has a host table in the ** style GW terminal 1. A table comprises two or more records which used an extension terminal 2a-2n person as the key, and has a real IP address and a local IP address for VPNNAT as the field. In an initial state, a host table is empty.
[0116](10) VPNGW5 (5a-5n) on the maintenance server 3 enables existence of plurality. One VPNGW5 enables composition of two or more VPN tunnels 12 which the VPNGW5 permits.
(11) On the maintenance server 3, it has a VPNGW tunnel table. A table comprises two or more records which used the IP address and VPN tunnel number of VPN gateway 5 as the key, is assigned as a value of the field, and has the ** style GWID.
[0117][Explanation of a processing sequence] Details are hereafter explained about the procedure of each processing using drawing 3 - drawing 9, and drawing 12 - drawing 25. Number n-n (n is arbitrary natural numbers) currently shaken at the left in the letter corresponds to the step treating number in a figure.
[0118]the notice of installation, [being shown in <notice processing of installation> drawing 3, drawing 12 and drawing 13, and] It notifies the maintenance server 3 that the terminal 1 was installed, and they are the common informations (IPsec) for remote maintenance from the maintenance server 3. [PresharedKey and] It is the purpose to encipher and receive terminal 1 authentication password (following, Secret (ID2)) and a maintenance-man password, and to set it up.
[0119]using Secret (ID2) for the terminal authenticating processing after the notice processing of installation instead of Secret (ID) -- the terminal 1 --- those who used Secret (ID2) from Secret (ID) common to all are because SEKYURITI is strengthened. VPNNAT processing is performed, in order to avoid it since duplication of each ** style GW terminal 1 subordinate's private IP address can be considered when building VPN. It is the 2nd purpose to receive the straw-man private IP address for VPN for that (local IP address for the following and VPNNAT) from the maintenance server 3.
[0120]** Installation notice commands (terminal server part 10 -> maintenance center 9) (Communication opportunity) 1-1 After the end of terminal 1 installation, the router section 11 carries out by button grabbing to the server part 10, when the connections set of Internet 6 HE is completed. What is necessary is to perform the notice of installation only once.
[0121](Terminal pretreatment) The command sending-out treating part 103 of the 1-2 server part 10 generates a secret key and a public key. Public key encryption, such as RSA, is used for an algorithm.
1-3 Create the original text for attestation from "unique ID+ time stamp of the terminal 1."
1-4 Generate the message attestation child (MAC) using Secret (ID) to the original text (being based on ISO9797-1 and ISO9797-2 is desirable).
[0122](Command transmission processing) 1-5 Terminal ID, a public key, the original text, and MAC are made into a parameter, Installation notice commands are transmitted as a <non-IPsec session> by the http command from the terminal 1 (server part 10 / command sending-out treating part 103) to the maintenance server 3 (http server part 30).
[0123]** Notice response of installation (maintenance server 3 -> terminal server part 10) (Maintenance server process) 1-6 the http server part 30 of the maintenance server 3, The command name and parameter which were received are passed to the CGI treating part 31, and it checks that the CGI treating part 31 generates the message attestation child (MAC) using Secret (ID) (the same operation as the terminal 1), and is in agreement with MAC which received to the original text (terminal attestation).

[0124]The CGI treating part 31 1-7 The authentication key of IPsec (Preshared Key), Secret (ID2) is generated at random, a maintenance-man password is acquired from a configuration file, the record corresponding to terminal ID in terminal 1DB is created newly (it overwrites, when it already exists), and it holds in each field of an applicable record.
[0125]1-8 The CGI treating part 31 is vacant from VPNNATDB91, and chooses the local IP address for VPNNAT as the object for the server parts 10, and the two router sections 11, While holding ** style GW terminal ID / terminal name in the quota situation field of an applicable record, the local IP address for VPNNAT is held to the local IP address for server part 10VPNNAT of terminal 1DB, and the local IP address field for router section 11VPNNAT.
[0126]1-9 The CGI treating part 31 enciphers the authentication key (Preshared Key) of IPsec, Secret (ID2), a maintenance-man password, the server part 10, and the local IP address for VPNNAT for the router sections 11 by the public key of the ** style GW terminal 1.
[0127](Response transmitting processing) 1-10 the http server part 30 of the maintenance server 3, Status (normal or error statuses (abnormalities in attestation, etc.)), the authentication key of IPsec enciphered by the public key of the terminal 1 (Preshared Key), Secret (ID2) enciphered by the public key of the terminal 1, the maintenance-man password enciphered by the public key of the terminal 1, The local IP address for VPNNAT for server parts enciphered by the public key of the terminal 1, The data which made the parameter the local IP address for VPNNAT for router sections enciphered by the public key of the terminal 1 is received from the CGI treating part 31, A response is transmitted as a http response <non-IPsec session> from the maintenance server 3 (http server part 30) to the terminal 1 (server part 10 / command sending-out treating part 103).
[0128]** VPNNAT110 setting out of the server part 10 and the router section 11 (terminal server part 10 -> terminal router section 11)
(Terminal post-processing) The 1-11 terminal-server part 10, With the secret key of the terminal 1, the authentication key (Preshared Key) of IPsec, Secret (ID2), the password for maintenance men, the local IP address for VPNNAT for server parts, and the local IP address for VPNNAT for router sections are decrypted and held.
[0129]1-12 Preshared Key which the terminal server part 10 made VPN gateway 5 with IPsec object hosts, The setting command (it changes with mounting of the telnet command of the router section 11) of the local IP address for VPNNAT for server parts and the local IP address for VPNNAT for router sections is created. At this time, the address of a VPN gateway is set up with a straw man.
[0130](Command transmission processing) 1-13 A command is sent out by making into a parameter the command created by pre- processing as a telnet command <local network session> from a terminal (router setting processing part 102) to the terminal 1 (router section 11).
(Terminal router section processing) 1-14 Setting out of Preshared Key and setting out of VPNNAT110 which were received are written in the router section 11.
[0131](Response transmitting processing) 1-15 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <non-IPsec session> from the terminal 1 (router section 11) to the terminal 1 (server part 10 / command sending-out treating part 103).
(Terminal router set part post-processing) The notice processing of installation is completed by the nothing above.
[0132]Failure information processing detects that the terminal 1 broke down, and notifies it to the maintenance server 3 so that the sequence diagram of <failure information processing> drawing 26 and the procedure figure of the process flow of drawing 27 may be shown. In the terminal 1 (server part 10), generating of failure of the server part 10 of the terminal 1 and the router section 11 and restoration are monitored continuously, and if failure occurs, failure information processing will be started. That is, ** failure information command (terminal ID, original text, MAC, failure code) ->** failure information response ->** remote maintenance demand starting of failure information processing is performed.
[0133](Communication opportunity) 7-1 When a failure occurrence is detected at the terminal 1,

the terminal 1 carries out autonomously.
(Terminal pretreatment) 7-2 The original text for attestation is created from "unique ID+ time stamp of the terminal 1."
7-3 Generate the message attestation child (MAC) using Secret (ID2) to the original text (being based on ISO9797-1 and ISO9797-2 is desirable).
[0134](Command transmission processing) 7-4 Terminal ID, the original text, MAC, and the code of failure are made into a parameter, A failure information command is transmitted as a <non-IPsec session> by the http command from the terminal 1 (server part 10 / command sending-out treating part 103) to the maintenance server 3 (http server part 30).
[0135](Maintenance server process) 7-5 The http server part 30 of the maintenance server 3 passes the command name and parameter which were received to the CGI treating part 31. It checks that the CGI treating part 31 generates the message attestation child (MAC) using Secret (ID2) (the same operation as the terminal 1), and is in agreement with MAC which received to the original text (terminal attestation).
7-6 The CGI treating part 31 holds the received failure code.
[0136](Response transmitting processing) 7-7 the http server part 30 of the maintenance server 3, The data which made the parameter status (normal or error statuses (abnormalities in attestation, etc.)) is received from the CGI treating part 31, A response is transmitted as a http response <non-IPsec session> from the maintenance server 3 (http server part 31) to the terminal 1 (server part 10 / command sending-out treating part 103).
[0137](Terminal post-processing) 7-8 VPNGW address request processing is started.
It is desirable that the failure code held by failure information processing can be referred to by http access etc. from the remote maintenance device 4 (failure confirming processing).
[0138]Like the sequence diagram of <VPNGW address request processing> drawing 4 and drawing 14, and the process flow procedure of drawing 15, a VPNGW address request makes it main point to notify the address of VPN gateway 5i of the maintenance center 9 which the maintenance server 3 chose to the ** style GW terminal 1. Although a VPNGW address request is fundamentally notified when the ** style GW terminal 1 has registration of a remote maintenance demand from the extension terminals 2a-2n, a terminal management person is also enabled to notify a VPNGW address request by button grabbing of ** style GW terminal 1 main part.
[0139]** VPNGW address request command (terminal server part 10 -> maintenance server 3)
(Communication opportunity)
9-1 It is based on action to the ** style GW terminal 1 by WEB access to the ** style GW terminal 1 from the extension terminals 2a-2n, or a terminal management person's button grabbing.
[0140](Terminal pretreatment)
9-2 When started by browser access from the extension terminals 2a-2n, By making "the claimant name, the claimant level, the extension terminal name (multidata input is good), the urgency, telephone number, and request content" which are information required of a remote maintenance demand input from a browser, it acquires and holds as remote maintenance information. In a screen image, it is as a browser picture. When started by button grabbing of the ** style GW terminal 1, "a claimant name, a claimant level, a terminal name, urgency, a telephone number, and a request content" are acquired from the table registered a priori, and are held. A claimant level enables [general or] setting out of an administrator. An extension terminal name is a name of an extension terminal to make into a remote maintenance object, and other information, the user to whom the operator of the maintenance center 9 started the remote maintenance demand carries out remote maintenance to the operator of the center 9 -- I have you -- it is information to hit and for the intention to be shown.
[0141]9-3 The command sending-out treating part 103 of the server part 10 generates a secret key and a public key. Public key encryption, such as RSA, is used for an algorithm.
9-4 Generate the original text for attestation from "unique ID+ time stamp of a terminal."
9-5 Generate the message attestation child (MAC) using Secret (id2) to the original text. Being based on (ISO9797-1, ISO9797-2) is desirable.

[0142](Command transmission processing)
9-6 Transmit a remote maintenance demand command as a <non-Ipsec session> by the http command from the terminal 1 (server part 10 / command sending-out treating part 103) to the maintenance server 3 (http server part 30) by making terminal ID, the original text, MAC, and a public key into a parameter.
[0143]** VPNGW selection process (maintenance server treating part)
9-7 The http server part 30 of the maintenance server 3 passes the command name and parameter which were received to the CGI treating part 31. It checks that the CGI treating part 31 generates the message attestation child (MAC) using Secret (id2) (the same operation as the terminal 1), and is in agreement with MAC which received to the original text. (Terminal attestation)
[0144]9-8 The maintenance server 3 reads the VPNGW tunnel DB, search the tunnel of the quota situation of the VPNGW tunnel DB from a head, and the value of the field acquires an "intact" tunnel number. The field corresponding to the acquired tunnel number concerned is rewritten from "it is intact" to "terminal ID", and a corresponding VPNGW global IP address is acquired. Hereafter, VPNGW corresponding to this global IP address is set to "5i." A VPN gateways [which were shown here / 5a-5n] selection process is one of the features of this invention.
[0145]9-9 Encipher by the public key which received the above "VPNGW global IP address" of the parameter of a response.
[0146]** VPNGW address request response (maintenance server 3 -> terminal server part 10)
(Response transmitting processing)
9-10 The http server part 30 of the maintenance server 3, The data which made the parameter status (normal or error statuses (abnormalities in attestation, etc.)) and the VPNGW global IP address enciphered by the public key of the terminal 1 is received from the CGI treating part 31, A response is transmitted as a http response <non-session> from the maintenance server 3 (http server part 30) to the terminal 1 (server part 10 / command sending-out treating part 103).

[0147]** VPNNG address request response receiving post-processing (terminal server part 10 -> terminal router section 11)
(Terminal pretreatment)
9-11 The terminal server part 10 is a secret key of the terminal 1, and decrypts and holds a VPNGW global IP address.
[0148]9-12 The terminal server part 10 creates the command (it changes with mounting of the telnet command of the router section 11.) for setting up a VPNGW global IP address as a VPN opposite host.
9-13 Send out a command by making into a parameter the command created by pre- processing as a telnet command <local network session> from the terminal 1 (router setting processing part 102) to the terminal 1 (router section 11).
[0149](Terminal router section processing)
9-14 Write setting out which makes a VPNGW global address a VPN opposite host in the router section 11.
(Response transmitting processing)
9-15 Transmit a response as a telnet response <non-Ipsec session> from the terminal 1 (router section 11) to the terminal 1 (server part 10 / command sending-out treating part 103) by making status (normal or error statuses (abnormalities in a command, etc.)) into a parameter.
[0150](Terminal router set part post-processing)
9-16 Start a remote maintenance request process.
VPNGW address request processing is completed by the above. This the processing of this is one of the points of an invention.
[0151]As shown in the procedure figure of the process flow of the sequence diagram of <remote maintenance request process> drawing 5, drawing 16, or drawing 19, a remote maintenance request process makes it main point to require implementation of the remote maintenance by IPsec of the maintenance server 3.

[0152]It is also one of the main point to notify the IP address of the ** style GW terminal 1 for building VPN to the center 9 in a remote maintenance request process. A remote maintenance demand is performed by the http protocol and the maintenance server 3 acquires the IP address received to the ** style GW terminal 1 from the environment variable. A VPN key and a terminal IP address are set up to VPN gateway 5i of the maintenance center 9 based on the IP address.
[0153]When building VPN, in order to enable it to communicate IP level to each ** style GW terminal 1 subordinate's extension terminals 2a-2n, the local IP address for VPNNAT to the extension terminals 2a-2n for remote maintenance is acquired from the center 9, and VPNNAT processing is performed.
[0154]Even when performing the maintenance to two or more ** style GW terminals 1 with ** style GW terminal 1 subordinate's same local LAN address by performing VPNNAT processing. (In for example, the case so that the two ** style GW terminals 1 of a maintenance object may exist and both the two ** style GW terminals 1 may have 192.168.0.0/24 of local networks). as opposed to the ** style GW terminal 1 from an operator terminal of the maintenance center 9, and the subordinate's extension terminals 2a-2n -- IP -- RICHABURU environment can be built.

[0155]** Remote maintenance demand command (terminal server part 10 -> maintenance server 3)
(Communication opportunity) It is started after the end of processing of a 2-1 VPNGW address request.
[0156](Terminal pretreatment) The remote maintenance information held by the 2-2 VPNGW address request is acquired.
[0157]2-3 The command sending-out treating part 103 of the server part 10 generates a secret key and a public key. Public key encryption, such as RSA, is used for an algorithm.
2-4 Create the original text for attestation from "unique ID+ time stamp of the terminal 1."
[0158]2-5 Generate the message attestation child (MAC) using Secret (ID2) to the original text (being based on ISO9797-1 and ISO9797-2 is desirable).
2-6 Encipher "a claimant name, an extension terminal name, a telephone number, and a request content" by Secret (ID2) currently held at the ** style GW terminal 1 among the parameters for notifying to the maintenance center 9.
[0159](Command transmission processing) 2-7 Terminal ID, the original text, MAC, a public key, a claimant level, urgency, an encryption claimant name, an encryption extension terminal name (plurality is good), an encryption telephone number, and an encryption request content are made into a parameter, A remote maintenance demand command is transmitted as a <non-IPsec session> by the http command from the terminal 1 (server part 10 / command sending-out treating part 103) to the maintenance server 3 (http server part 30).
[0160]** Local IP address quota processing (maintenance server process) 2-8 for VPNNAT The http server part 30 of the maintenance server 3 passes the command name and parameter which were received to the CGI treating part 31. It checks that the CGI treating part 31 generates the message attestation child (MAC) using Secret (ID2) (the same operation as a terminal), and is in agreement with MAC which received to the original text (terminal attestation).
[0161]2-9 The CGI treating part 31 generates a number of acceptance, creates the record of remote maintenance demand DB92 newly, and holds a number of acceptance, the receipt time, and the Menten Nance state (this time always correspondence waiting) to terminal DB90 of a maintenance terminal browser. To a table name, when a claimant level is an administrator, it holds as an "administrator", and when a claimant level is general, the extension terminal 2a - a 2n person are held. The record of terminal DB90 is shown in drawing 26.
[0162]2-10 The CGI treating part 31 acquires the global IP address of the ** style GW terminal 1 from environment variable REMOTE_ADDR, and holds it on the record of said remote maintenance demand DB92.
2-11 The CGI treating part 31 holds terminal ID, a claimant level, and urgency on the record of said remote maintenance demand DB92.
[0163]2-12 The CGI treating part 31 decrypts an encryption extension terminal name, an encryption claimant name, an encryption telephone number, and an encryption request content

by Secret (ID2), and holds them on the record of said remote maintenance demand DB92. The record of remote maintenance demand DB92 is shown in drawing 27.
[0164]2-13 The CGI treating part 31 searches VPNNATDB91 by using notified terminal ID / extension terminal name (when two or more terminal names exist, it is about each terminal name) as a key, and judges whether the local IP address for VPNNAT is assigned to the terminal 1.
[0165]If the local IP address for VPNNAT is assigned, the assigned local IP address for VPNNAT will be held on the record of said remote maintenance demand DB92, If the local IP address for VPNNAT is not assigned, it is vacant from VPNNATDB91 and the local IP address for VPNNAT is chosen.
[0166]While holding ** style GW terminal ID / extension terminal name in the quota situation field of an applicable record, the held local IP address for VPNNAT is held also on the record of said remote maintenance demand DB92. The record of VPNNATDB91 is shown in drawing 30.
[0167]2-14 The CGI treating part 31 creates a page so that it can indicate that it received the remote maintenance demand on the WEB browser of the remote maintenance device 4. Display information displays a number of acceptance, terminal ID, a global IP address, a claimant name, a claimant level, a telephone number, urgency, a request content, the receipt time, the local IP address for VPNNAT, a table name, and a maintenance state (refer to drawing 29).
[0168]** Remote maintenance demand response processing (maintenance server 3 -> terminal server part 10)
(Maintenance server part)
2-26 Encipher by the public key which received "the group of an extension terminal name and a straw-man IP address" among response processings.
(Response transmitting processing)
2-27 The http server part 30 of the maintenance server 3, Status (normal or error statuses (abnormalities in attestation, etc.)), a number of acceptance, The data which made the parameter the group (plurality is good) of the extension terminal name enciphered by the public key of the terminal 1 and the local IP address for VPNNAT is received from the CGI treating part 31, A response is transmitted as a http response <non-Ipsec session> from the maintenance server 3 (http server part 30) to the terminal 1 (server part 10 / command sending-out treating part 103).

[0169]** IPsec processing-object packet setting out (maintenance center 9 -> VPN gateway 5i)
(Command transmission processing)
2-15 The VPN gateway setting processing part 32 acquires the packet for local IP addresses for VPNNAT held by processing of terminal ID and ** from the applicable record of the remote maintenance demand DB.
2-16 The VPN gateway setting processing part 32, Setting out (it changes with mounting of the telnet command of VPN gateway 5i.) for assigning the packet for local IP addresses for VPNNAT to VPN tunnel 12 corresponding to terminal ID is made into a parameter, A command is transmitted as a telnet command <local network session> from the maintenance server 3 (VPN gateway setting processing part 32) to VPN gateway 5i (setting command receiving processing part 51).
[0170](VPN gateway processing)
2-17 Write setting out for making the received local IP address for VPNNAT into an IPsec processing-object host in VPN gateway 5i.
(Response transmitting processing)
2-18 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <local network session> from VPN gateway 5i (setting command receiving processing part 51) to the maintenance server 3 (VPN gateway setting processing part 32).
[0171](VPN gateway setting processing part post-processing)
2-19 The VPN gateway setting processing part 32 acquires whether VPN is established between the ** style GW terminals 1 with terminal ID which received by "** remote maintenance demand command" from VPN gateway 5i.

2-20 From the VPN establishment situation of VPN gateway 5i, when VPN is established, end a process. When VPN is not established, **IPsec setting processing is started.
[0172]** IPsec setting processing (maintenance center 9 -> VPN gateway 5i)
(VPN gateway setting processing part pretreatment)
2-21 Acquire the authentication key (PresharedKey) of IPsec, and the global IP address of the terminal router section 11 from the maintenance server 3/the CGI treating part 31, and generate a command.
[0173](Command transmission processing)
2-22 Setting out for establishing VPN tunnel 12 corresponding to setting out and terminal ID of Presharedkey which made the global IP address of the terminal router section 11 IPsec object hosts (by mounting of the telnet command of VPN gateway 5i.) It differs. It is considered as a parameter and a command is transmitted as a telnet command <local network session> from the maintenance server 3 (VPN gateway setting processing part 32) to VPN gateway 5i (setting command receiving processing part 51).
[0174](VPN gateway processing)
2-23 Write setting out for establishing Presharedkey and VPN tunnel 12 which were received in VPN gateway 5i.
(Response transmitting processing)
2-24 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <local network session> from VPN gateway 5i (setting command receiving processing part 51) to the maintenance server 3 (VPN gateway setting processing part 32).
[0175](Maintenance server post-processing)
2-25 The VPN gateway setting processing part 32 acquires whether establishment of VPN is completed between the ** style GW terminals 1 with terminal ID which received by "** remote maintenance demand command" from VPN gateway 5i. When establishment is not completed, the same acquisition processing is repeated until it checks completion of VPN establishment at intervals of several seconds. When the completion of establishment of VPN is able to be checked, ** remote maintenance demand response processing is started. It is desirable for the state to be able to check from the remote maintenance device 4 in the stage which VPN setting out completed. A reason is because it is [a maintenance man's working efficiency] better to have been able to perform ** remote maintenance start indication, after checking that VPN setting out had been completed.
[0176]** VPNNAT setting out of the server part 10 and the router section 11 (terminal server part 10 -> terminal router section 11)
(Terminal treatment part)
2-28 The terminal server part 10 which received the remote maintenance demand response holds a number of acceptance.
2-29 The terminal server part 10 is a secret key of the terminal 1, decrypts the group (in the cases of two or more ****) of an extension terminal name and the local IP address for VPNNAT, and holds it to a host table.
[0177]2-30 the terminal server part 10 uses an extension terminal name as a key -- the terminal server part 10 -- with, the real IP address corresponding to a terminal name from the table (see by DNS etc.) of the group of the extension terminal name which is, and a real IP address, [acquire and] The setting command (in the cases of two or more ****) (it changes with mounting of the telnet command of the router section 11.) which matches the local IP address for VPNNAT and real IP address corresponding to a terminal name by VPNNAT110 is created.
(Command transmission processing)
2-31 Send out a command by making into a parameter the command created by 2-30 as a telnet command <local network session> from the terminal 1 (router setting processing part 102) to the terminal 1 (router section 11).
[0178](Terminal router section processing)
2-32 Write setting out of VPNNAT110 in the router section 11.
(Response transmitting processing)

2-33 Transmit a response as a telnet response <non-Ipsec session> from the terminal 1 (router section 11) to the terminal 1 (server part 10 / command sending-out treating part 102) by making status (normal or error statuses (abnormalities in a command, etc.)) into a parameter. (Terminal router set part post-processing) A remote maintenance request process is completed by more than nothing.

[0179]As shown in the sequence diagram of <remote maintenance implementation processing> (remote maintenance device 4 -> extension terminalsa [2]-2n) drawing 6, and the procedure flow chart of drawing 19, Remote maintenance implementation processing receives said remote maintenance request process, Secure remote maintenance is performed from the remote maintenance device 4 to ** style GW terminal 1 main part and its extension terminals 2a-2n via the tunnel 12 by VPN, such as IPsec (in order to carry out via VPN). Let it be main point to carry out restoration of the failure of the terminal 1 which can encipher a transmission line, remote installation of the application of PASOKONHE, etc.

[0180]The remote maintenance device 4 is not special, and by sending out a command to the extension terminals 2a-2n on the local network 8, if it is a device which can maintain the extension terminals 2a-2n, it can divert it to some other purpose. As a function, about failure (for example, Proxy failure), restoration operation (starting of proxy, reboot of the terminal 1) is performed, and failure is restored. The display of the log of the terminal 1 and the check of setting out of the router section 11 can also be performed. As a tool, they are a http client (WeB browser), a telnet tool, etc.

[0181]About remote installation to a personal computer, it is based on remote-control software, such as VNC, etc. Therefore, since this processing is a general-purpose thing depending on the communications protocol from the remote maintenance device 4 to the extension terminals 2a-2n which perform a maintenance, it does not make reference in detail.

[0182]Although it becomes a repetition, it is a point of this example of an embodiment to make connection with the extension terminals 2a-2n from the center 9 to the local IP address for VPNNAT given to the remote maintenance demand.

[0183]** In the state where remote maintenance start processing (remote maintenance device 4 -> maintenance server 3 (communication opportunity)) VPN tunnel 12 is stretched, From the WEB browser on the remote maintenance device 4 (maintenance terminal in a figure), it is started by a remote maintenance maintenance man's arbitrary opportunities (even when failure is detected by the failure confirming processing mentioned above, starting synchronizing with it is desirable).

[0184](Remote maintenance start processing) 3-1 The remote maintenance demand confirmation screen of the maintenance server 3 is accessed, and it is notified to the maintenance server 3 by the CGI treating part 31 that the remote maintenance to the target remote maintenance demand was started.

[0185](Server process) If a remote maintenance start is started by the 3-2 CGI treating part 31, the maintenance state of the applicable table of remote maintenance demand DB92 will become "under correspondence."

[0186]** Remote maintenance implementation processing (remote maintenance device 4 -> extension terminals 2a-2n)

(Remote Menten Nance operation) 3-3 Remote maintenance is carried out. In remote maintenance, an IP connection is performed via VPN to the local IP address for VPNNAT which received the remote maintenance demand. At the time of remote maintenance implementation, it recommends strongly designing the user interface by the side of a server work referring to remote maintenance demand DB92.

[0187]As shown in the sequence diagram of <remote maintenance end-processing> drawing 7, and the procedure flow chart of drawing 20, remote maintenance end processing, Let it be main point to tell that the remote maintenance work demanded by the remote maintenance demand was completed to the ** style GW terminal 1 from the maintenance server 3.

[0188]** Remote maintenance quit-command transmitting processing (maintenance server 3 -> terminal server part 10)

(Communication opportunity) When the demanded remote maintenance work is completed in the

state where 4-1 VPN tunnel 12 is stretched, It is started from the WEB browser on the remote maintenance device 4 by the kick of the CGI treating part 31 by the remote maintenance maintenance man to the maintenance server 3.
[0189](Server pretreatment) If the end of remote maintenance is started by the 4-2 CGI treating part 31, the maintenance state of the applicable table of remote maintenance demand DB92 will be "ended." The table record of remote maintenance demand DB92 is shown in drawing 31.
[0190]4-3 as for the maintenance server 3, the maintenance state of the applicable table of remote maintenance demand DB92 was "ended", if thing detection is carried out, The number of acceptance of an applicable table is acquired by making ********** into a parameter, and a remote maintenance quit command is created by using a number of acceptance as bara meter. The VPNNAT110 release processing and VPN end processing which explain this number of acceptance later are also referred to.
[0191](Command transmission processing) 4-4 A remote maintenance quit command is transmitted as a <IPsec session> by making into a parameter the command created by pre-processing by the http command from the maintenance server 3 to the terminal 1 (http server part 100).
[0192]** Remote maintenance quit-command reception (terminal server part 10 -> maintenance server 3)
(Terminal server part processing) 4-5 If the end of remote maintenance is received, a number of acceptance will be extracted from a parameter and the state of the number of acceptance currently held will be considered as an end.
[0193](Response transmitting processing) 4-6 The http server part 100 of the terminal 1 makes status (normal or error status) a parameter, and transmits a response as a http response <IPsec session> of maintenance center 9 HE from the terminal 1 (http server part 100).
[0194]** End response of remote maintenance receiving post-processing (maintenance server 3)

(Server post-processing) 4-7 It judges whether all maintenances to the applicable extension terminals 2a-2n were completed after response reception, and processing will be ended if all maintenances to the applicable extension terminals 2a-2n are not completed. All maintenances to the applicable extension terminals 2a-2n judge the server part 10 or the router section 11 of the ** style GW terminal 1, and end ****** et al. and the extension terminal ended further start VPNNAT release processing, when it is not the server part 10 or the router section 11 of the terminal 1.
[0195]In the case of the server part 10 of the terminal 1, or the router section 11, if it judged whether all the remote maintenance to the corresponding ** style GW terminal 1 was ended and has all ended, VPN end processing will be started, and processing will be ended if it all has not ended. Above, remote maintenance end processing is completed.
[0196]As shown in the sequence diagram of <VPNNAT release processing> drawing 8 and drawing 21, and the procedure flow chart of drawing 22, VPNNAT110 release processing, Let it be main point to release the local IP address for VPNNAT for VPNNAT assigned to the remote maintenance demand by the ** style GW terminal 1 from the maintenance center 9.
[0197]** VPNNAT110 release command transmission processing (maintenance server 3 -> terminal server part 10)
(Communication opportunity) In the state where 5-1 VPN tunnel 12 is stretched, all maintenances to the applicable extension terminals 2a-2n are completed after the end of remote maintenance, and when the extension terminals 2a-2n are except server part [of the ** style GW terminal 1] 10, or router section 11, it is started.
[0198](Server pretreatment) A 5-2 VPNNAT110 release command is created. The table record of remote maintenance demand DB92 is the same as that of drawing 31.
(Command transmission processing) 5-3 The maintenance server 3 transmits a VPNNAT release command as a <IPsec session> by making an extension terminal name into a parameter by the http command from the maintenance server 3 to the terminal 1 (http server part 100).
[0199]** VPNNAT release command receiving process (terminal server part 10 -> terminal router section 11)

(Terminal pretreatment) The 5-4 terminal-server part 10, A VPNNNAT110 release command is received and the real IP address corresponding to a terminal name is acquired from the table (see by DNS etc.) of the group of the terminal name which the terminal server part 10 has, and a real IP address by using the extension terminal 2a-2n person of a parameter as a key.
[0200]And the command (in the cases of two or more ****) (it changes with mounting of the telnet command of the router section 11) which releases VPNNAT110 corresponding to a terminal name of the local IP address for VPNNAT and a real IP address is created.
[0201](Command transmission processing) 5-5 A command is sent out by making into a parameter the command created by pre- processing as a telnet command <local network session> from the terminal 1 (router setting processing part 102) to the terminal 1 (router section 11).
(Terminal router section processing) Setting out of 5-6 VPNNAT110 release is written in the router section 11.
[0202](Response transmitting processing) 5-7 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <non-IPsec session> from the terminal 1 (router section 11) to the terminal 1 (server part 10 / command sending-out treating part 103).
(Terminal router set part post-processing) 5-8 The record corresponding to the terminal name of a host table is deleted.
[0203]** VPNNAT110 release response transmitting processing (terminal server part 10 -> maintenance server 3)
(Response transmitting processing) 5-9 The http server part 100 of the terminal 1 makes status (normal or error status) a parameter, and transmits a response as a http response <IPsec session> of maintenance center 9 HE from the terminal 1 (server part 10).
[0204]** Local IP address translation processing for maintenance server side VPNNAT (maintenance server 3)
(Local IP address translation processing for VPNNAT) 5-10 While acquiring the local IP address for VPNNAT corresponding to the extension terminals 2a-2n corresponding to the number of acceptance under processing from remote maintenance demand DB92 and holding it by the server side, The local IP address for correspondence VPNNAT of VPNNATDB91 is released.
[0205]** IPsec processing-object packet release setting out (maintenance server 3 -> VPN gateway 5)
(Command transmission processing) The 5-11 VPN-gateway setting processing part 32 acquires terminal ID and the local IP address for VPNNAT from the record applicable to the number of acceptance under processing of remote maintenance demand DB92.
[0206]5-12 The VPN gateway setting processing part 32, The command (it changes with mounting of the telnet command of VPN gateway 5) for canceling setting out for assigning the packet for local IP addresses for VPNNAT to VPN tunnel 12 corresponding to terminal ID is made into a parameter, A command is transmitted as a telnet command <local network session> from the maintenance server 3 (VPN gateway setting processing part 32) to VPN gateway 5 (setting command receiving processing part 51).
[0207](VPN gateway processing) 5-13 Setting out of received routing for local IP addresses for VPNNAT is canceled of VPN gateway 5.
[0208](Response transmitting processing)
5-14 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <local network session> from VPN gateway 5 (setting command receiving processing part 51) to the maintenance server 3 (VPN gateway setting processing part 32).
[0209](VPN gateway setting processing part post-processing) 5-15 Processing will be ended if VPN end processing would be started and it will all have ended, if it judged whether all the remote maintenance to the corresponding ** style GW terminal 1 was ended and has all ended, and it is not.
[0210]As shown in the sequence diagram of <VPN end-processing> drawing 9 and drawing 23 thru/or the procedure flow chart of drawing 25, VPN end processing makes it main point to end

VPN built by the remote maintenance demand from the maintenance center 9.
[0211]** VPN quit-command transmitting processing (maintenance server 3 -> terminal server part 10)
(Communication opportunity) In the state where 6-1 VPN tunnel 12 is stretched, when all maintenances to the corresponding ** style GW terminal 1 are completed after the end of remote maintenance, it is started.
[0212](Server pretreatment) A 6-2 VPN quit command is created. The table record of remote maintenance demand DB92 is the same as that of drawing 29.
(Command transmission processing)
6-3 The maintenance server 3 transmits a VPN quit command as a <IPsec session> by the http command from the maintenance server 3 to the terminal 1 (http server part 100).
[0213]** VPN quit-command reception (terminal server part 10 -> terminal router section 11)
(Terminal pretreatment) The 6-4 terminal-server part 10 receives a VPN quit command, and creates the command (in the cases of two or more ****) (it changes with mounting of the telnet command of the router section 11) which releases all the VPNNAT110.
[0214](Command transmission processing) 6-5 A command is sent out by making into a parameter the command created by pre- processing as a telnet command <local network session> from the terminal 1 (router setting processing part 102) to the terminal 1 (router section 11).
** VPNNAT setting-out initialization-commands reception and processing (router section 11)
(Terminal router section processing) Setting out of 6-6 VPNNAT110 release is written in the router section 11.
[0215](Response transmitting processing) 6-7 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <local session> from the terminal 1 (router section 11) to the terminal 1 (server part 10 / command sending-out treating part 103).
(Terminal router set part post-processing) 6-8 All host tables are deleted.
[0216]** End response of VPN transmitting processing (terminal server part 10 -> maintenance server 11)
(Response transmitting processing) 6-9 The http server part 100 of the terminal 1 makes status (normal or error status) a parameter, and transmits a response as a http response <IPsec session> of maintenance center 9 HE from the terminal 1 (http server part 100).
[0217]** Local IP address translation processing for maintenance server side VPNNAT (maintenance server 3)
(Local IP address translation processing for VPNNAT) 6-10 While acquiring all the local IP addresses for VPNNAT corresponding to the number of acceptance under processing from remote maintenance demand DB92 and holding them by the server side, The local IP address for correspondence VPNNAT of VPNNATDB91 is released.
[0218]** IPSec processing-object packet release setting out (maintenance server 3 -> VPN gateway 5)
(Command transmission processing) The 6-11 VPN-gateway setting processing part 32 acquires all the terminal ID corresponding to terminal ID, and local IP addresses for VPNNAT from the applicable record of remote maintenance demand DB92.
[0219]6-12 The VPN gateway setting processing part 32, The command (it changes with mounting of the telnet command of VPN gateway 5) for canceling setting out for assigning the packet for local IP addresses for VPNNAT to VPN tunnel 12 corresponding to terminal ID is made into a parameter, A command is transmitted as a telnet command <local network session> from the maintenance server 3 (VPN gateway setting processing part 32) to VPN gateway 5 (setting command receiving processing part 51).
[0220](VPN gateway processing) 6-13 Setting out of received routing for local IP addresses for VPNNAT is canceled of VPN gateway 5i.
[0221](Response transmitting processing) 6-14 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <local network session> from VPN gateway 5 (setting command receiving processing part 51) to

the maintenance server 3 (VPN gateway setting processing part 32).
[0222]** IPsec reset command transmission processing (maintenance server 3 -> VPN gateway 5)
(Command transmission processing) The 6-15 VPN-gateway setting processing part 32 acquires terminal ID from the record of remote maintenance demand DB92 corresponding to the number of acceptance under processing.
[0223]6-16 The VPN gateway setting processing part 32, Setting out (it changes with mounting of the telnet command of VPN gateway 5) for canceling VPN tunnel 12 corresponding to terminal ID is made into a parameter, A command is transmitted as a telnet command <local network session> from the maintenance server 3 (VPN gateway setting processing part 32) to VPN gateway 5 (setting command receiving processing part 51).
[0224]** IPsec reset command reception and processing (VPN gateway 5)
(VPN gateway processing) 6-17 Setting out of VPN corresponding to terminal ID which received is canceled of VPN gateway 5.
[0225](Response transmitting processing) 6-18 Status (normal or error statuses (abnormalities in a command, etc.)) is made into a parameter, A response is transmitted as a telnet response <local network session> from VPN gateway 5 (setting command receiving processing part 51) to the maintenance server 3 (VPN gateway setting processing part 32).
[0226](VPN gateway setting processing part post-processing) The field which carried out acquisition maintenance from the VPN gateway tunnel DB by 6-19 VPNGW address request processing, and wrote in "terminal ID" is rewritten "for it to be intact", and a VPN tunnel resource is released.
Remote maintenance end processing is completed by the above. In the above, the procedure of remote maintenance was explained based on the sequence diagram 3 - the sequence diagram 9 and the procedure flow chart 13 - the procedure flow chart 25.
[0227]The example of main story recording media makes free nonfiction of the computer reading of a series of conclusion procedure of the processing program procedure of the remote maintenance concerned.
[0228]Although setting out of VPNNAT110 to the server part 10 and the router section 11 of ** style GW terminal 1 main part is performed in this example of an embodiment at the time of the notice of installation, This is a function for enabling VPN access without a remote maintenance demand by arbitrary opportunities from the maintenance center 9 side at the ** style GW terminal 1. Therefore, it cannot be overemphasized that the procedure of setting VPNNAT110 as a remote maintenance demand and releasing it at the time of VPNNAT110 release without giving special treatment to setting out of VPNNAT110 to the server part 10 and the router section 11 of ** style GW terminal 1 main part may be sufficient.
[0229]In this example, although IPsec is used and explained to VPN, if this invention is VPN of layer 3 level, it cannot be overemphasized that it can apply also [except IPsec].
[0230]
[Effect of the Invention]According to this invention, the limited local IP address resource for VPNNAT used for VPNNAT in this way, By being assigned only to a remote maintenance request terminal and released in a VPNNAT release process at the time of the end of remote NANSU, IP address resources can be saved and the remote maintenance of many terminals can be simultaneously carried out as compared with a static VPNNAT method.
[0231]if it puts in another way — the former — the maximum — "— by using this invention to having become a remote maintenance object terminal about the extension terminal for local IP address resource" for VPNNAT, simultaneous — "— it becomes possible to use the extension terminal for local IP address resource" for VPNNAT as a remote maintenance object terminal, and the number of members of a remote maintenance service object terminal can be increased substantially.
[0232]And the limited local IP address resource for VPNNAT used for VPNNAT, By being assigned only to a remote maintenance request terminal and released in a VPNNAT release process at the time of the end of remote NANSU, The remote maintenance method which allows access from a maintenance center only to the extension terminal made applicable to a remote

maintenance demand is realizable.
[0233]For a remote maintenance purveyor of service, When a maintenance center installs equipment of a VPN gateway, according to the access number of VPN remote maintenance, extension installation of the equipment of a VPN gateway can be carried out, and the facility cost of a VPN gateway can be optimized by extension.
[0234]From the above-mentioned effect, for the visitor who enjoys remote maintenance service, when building a maintenance center and VPN, becoming the resource shortage of VPN decreases and the cases it becomes impossible to receive remote maintenance by VPN construction failure decrease in number.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－335273
（P2002－335273A）
(43)公開日　平成14年11月22日(2002.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ｈ　５Ｋ０３０
			Ｂ　５Ｋ０３３
12/46		12/46	Ａ

審査請求　未請求　請求項の数25　ＯＬ　（全 54 頁）

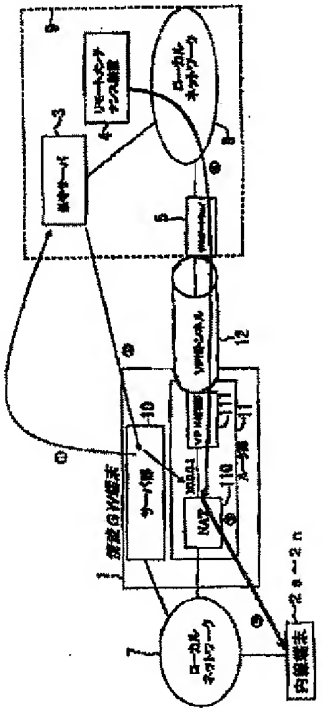
(21)出願番号　特願2001－350783(P2001－350783)
(22)出願日　平成13年11月15日(2001.11.15)
(31)優先権主張番号　特願2001－63453(P2001－63453)
(32)優先日　平成13年３月７日(2001.3.7)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　中濱　清志
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山田　敬信
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100071113
弁理士　菅　隆彦

Ｆターム(参考)　5K030 HA08 HD03 MA01 MD00
5K033 CB09 EC00

(54)【発明の名称】　リモートメンテナンス実施方法、システム及びプログラム並びにリモートメンテナンス実施プログラムを記録した記録媒体

(57)【要約】
【課題】保守センタからインターネットのＶＰＮ経由で、配下のローカルネットワークアドレスの重複を許容した複数の情流ＧＷ端末及びその内線端末に対して、同時に可能な限りリモートメンテナンスできる、リモートメンテナンス実施方法、プログラム及びシステム並びにリモートメンテナンス実施プログラムを記録した記録媒体の提供。
【解決手段】情流ＧＷ端末１におけるルータ部１１内に、そのローカルネットワーク７との間にＮＡＴ１１０を設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして保守センタ９から付与及び解放を行うことで実現する特徴的構成手法の採用。



【特許請求の範囲】
【請求項１】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行う実施方法であって、
前記それぞれのインターネットゲートウェイ端末におけるルータ部内に、そのローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタの保守サーバから付与及び解放を行うことにより前記リモートメンテナンスを実施する、
ことを特徴とするリモートメンテナンス実施方法。
【請求項２】前記実施方法における前記リモートメンテナンスの要求は、
当該要求を行う前記インターネットゲートウェイ端末が、リモートメンテナンス対象である内線端末名及び当該インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知すると、
当該通知を受けた当該保守サーバが、当該通知したリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該通知をしてきたインターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとしてレスポンスすると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において設置通知の際に共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を自己のＶＰＮゲートウェイに設定させ、当該ＶＰＮゲートウェイに対してＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを前記確立したＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行い、
前記レスポンスを受けたインターネットゲートウェイ端末が、受けた前記内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと前記ＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとし自己のルータ部に対して設定を行う、
以上の一連の処理を順次実施する、
ことを特徴とする請求項１に記載のリモートメンテナンス実施方法。
【請求項３】前記リモートメンテナンスの実施は、
前記リモートメンテナンス対象である前記内線端末に対して、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、前記保守センタから行われる、
ことを特徴とする請求項２に記載のリモートメンテナンス実施方法。
【請求項４】前記リモートメンテナンスの終了は、
先ず、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信し、
次に、当該送信を受けたサーバ部において、当該リモートメンテナンス終了コマンドに係る処理を行い、リモートメンテナンス終了レスポンスを送信し、
その後、当該リモートメンテナンス終了レスポンスを受信した保守サーバにて、該当内線端末に対するメンテナンスが全て終了したかの第１判断を行い、当該第１判断にて肯定の場合には当該終了した内線端末は前記インタネットゲートウェイ端末の前記サーバ部、前記ルータ部の何れかであるかの第２判断を行う一方、否定の場合には判断処理を終了し、当該第２判断にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行し、他方肯定の場合には対応する前記インタネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行するとともに否定の場合には当該判断処理を終了する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項２又は３に記載のリモートメンテナンス実施方法。
【請求項５】前記ＶＰＮＮＡＴ解放処理は、
先ず、前記保守サーバが、前記リモートメンテナンスの要求の際に設定した前記リモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、前記確立したＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する一方で、前記インターネットゲートウェイ端末に対して当該リモートメンテナンス対象の内線端末名を通知した後に、当該通知を受けたインターネットゲートウェイ端末が、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得して、それに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放し、
引続き、前記保守サーバが、前記第３判断を行いその判断結果に従う、
以上の一連の処理を順次実施する、
ことを特徴とする請求項４に記載のリモートメンテナンス実施方法。
【請求項６】前記ＶＰＮ終了処理は、
前記保守サーバが、ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に通知して、当該通知を受けたインターネットゲートウェイ端末が、当該ＶＰＮ終了コマンドに対する返答を当該保守サーバにＶＰＮ終了レスポンスとして送信し、

前記保守サーバが、前記ＶＰＮゲートウェイに、前記リモートメンテナンスの要求に際に設定した前記ＶＰＮトンネルを解除させ、当該ＶＰＮゲートウェイと前記インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項４又は５に記載のリモートメンテナンス実施方法。
【請求項７】前記設置通知は、
新たに設置された前記インターネットゲートウェイ端末の前記サーバ部から、当該設置について前記保守サーバに設置通知コマンドを通知し、
当該設置通知コマンドを受けた当該保守サーバにより、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスし、
当該レスポンスを受信した前記インターネットゲートウェイ端末は、ＩＰｓｅｃの認証鍵を自己の前記ルータ部に対して設定する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項２、３、４、５又は６に記載のリモートメンテナンス実施方法。
【請求項８】前記実施方法は、
前記リモートメンテナンスの要求、前記設定通知の何れか一方において、前記インターネットゲートウェイ端末の前記サーバ部及び前記ルータ部へのＶＰＮＮＡＴ設定処理を実施する、
ことを特徴とする請求項２、３、４、５、６又は７に記載のリモートメンテナンス実施方法。
【請求項９】前記実施方法は、
前記インターネットゲートウェイ端末に故障発生を検知した場合には、
先ず、当該インターネットゲートウェイ端末が、故障通知コマンドとして故障に係る情報を前記保守サーバに送信し、
次に、前記保守サーバが前記故障通知コマンドを受信すると当該故障に係る情報を処理して、当該故障通知コマンドを送信した前記インターネットゲートウェイ端末に故障通知レスポンスとして送信し、
更に、当該故障通知レスポンスを受信した当該インターネットゲートウェイ端末が前記リモートメンテナンスの要求に移行する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項２、３、４、５、６、７又は８に記載のリモートメンテナンス実施方法。
【請求項１０】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムであって、
前記インターネットゲートウェイ端末におけるルータ部内にそのローカルネットワークとＶＰＮ処理部との間にＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタから付与及び解放を行う機能構成にシステム構築する、
ことを特徴とするリモートメンテナンス実施システム。
【請求項１１】前記保守センタは、
前記インターネットゲートウェイ端末からリモートメンテナンス対象の内線端末名の通知を受けて当該リモートメンテナンス対象の内線端末名に対応するＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルアドレスの付与を行う保守サーバと、
前記リモートメンテナンスを行うリモートメンテナンス装置と、
当該リモートメンテナンス装置からの、当該リモートメンテナンス対象の内線端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスへアクセスを経由するＶＰＮゲートウェイとを、
保守センタローカルネットワークにてネットワーク構築する、
ことを特徴とする請求項１０に記載のリモートメンテナンス実施システム。
【請求項１２】前記インターネットゲートウェイ端末は、
前記保守センタにリモートメンテナンス対象の内線端末名を通知するサーバ部と、
当該通知したことにより当該保守センタから付与されたＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルＩＰアドレスと当該リモートメンテナンス対象の内線端末名のＩＰアドレスを割りつけるＶＰＮＮＡＴ及び当該保守センタの前記ＶＰＮゲートウェイとＶＰＮトンネルを確立するＶＰＮ処理部のルータ部とで構成して、
前記ＶＰＮゲートウェイを介した、リモートメンテナンス対象端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスへのアクセスにより、前記リモートメンテナンスを行うリモートメンテナンス装置からの、前記内線端末へのパケット転送を可能ならしめる機能を構築する、
ことを特徴とする請求項１０又は１１に記載のリモートメンテナンス実施システム。
【請求項１３】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを

確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末で用いられるプログラムであって、
当該インターネットゲートウェイ端末が設置された後に、リモートメンテナンスサービスを利用する場合に、前記保守センタに対して設置した旨を通知する設置通知処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、
前記設置について前記保守センタの保守サーバに設置通知コマンドを通知した後に、当該保守サーバからの当該設置通知コマンドに対するレスポンスを受信すると当該レスポンスとして受けたＩＰｓｅｃの認証鍵を自己のルータ部に対して設定する、
以上の一連の手順を踏む、ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１４】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、
当該インターネットゲートウェイ端末への、前記内部端末からのＷＥＢアクセス、当該インターネットゲートウェイ端末の操作者によるボタン操作の何れかにより、リモートメンテナンスを要求するリモートメンテナンス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、
リモートメンテナンス対象である前記内線端末名及び前記インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知した後に、
前記リモートメンテナンス要求コマンドに対するレスポンスを受けて、当該レスポンスとして受けた、内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと当該レスポンスとして受けたＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとして設定させる、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１５】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、
前記保守センタより行われる前記リモートメンテナンスの作業が終了した旨の通知に係るリモートメンテナンス終了処理を、当該通知を受けた前記インフェースゲートウェイ端末に行わせる前記プログラムの実行により、
前記保守センタからのリモートメンテナンス終了コマンドの受信を契機に、当該リモートメンテナンス終了コマンドに関する処理を行い、リモートメンテナンス終了レスポンスを送信して、
前記保守センタからＶＰＮ解放コマンドとしてリモートメンテナンス対象の内線端末名の通知を受けた場合には、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得し、取得した実ローカルＩＰアドレスに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１６】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、
前記リモートメンテナンスの要求に対応するリモートメンテナンス要求処理を前記保守サーバに行わせる前記プログラムの実行により、
前記要求を受けて、前記リモートメンテナンスの要求に係るリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該要求を行った前記インターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとして送信すると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を、自己のＶＰＮゲートウェイに指示し、自己の当該ＶＰＮゲートウェイに対して、ＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを、当該指示により確立されるＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行う、
以上の一連の手順を踏む、ことを特徴とするリモートメンテナンス実施プログラム。

【請求項１７】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該保守センタにて用いられるプログラムであって、
新たに設置された前記インターネットゲートウェイ端末からの設置通知コマンドを処理する設定通知コマンド処理を前記保守センタに行わせる前記プログラムの実行により、
前記設置通知コマンドに応じて、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスする、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１８】各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、
前記保守センタにおける終了ボタンが押されたことを契機に、前記リモートメンテナンスの作業が終了したことを通知するリモートメンテナンス終了処理を、前記保守サーバに行わせる前記プログラムの実行により、
ＶＰＮＮＡＴ用ローカルＩＰアドレスで確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信した後に、
当該リモートメンテナンス終了のレスポンスを受信すると、該当内線端末に対するメンテナンスが全て終了したかのを第１判断を行い、
当該第１判断にて肯定の場合には当該終了した前記内線端末は前記インターネットゲートウェイ端末の前記サーバ部かルータ部かの何れかであるかの第２判断を行う一方、否定の場合にはこのプログラムを終了し、
当該第２判断にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行する一方、肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、
当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行する一方、否定の場合にはこのプログラムを終了する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１９】前記ＶＰＮＮＡＴ解放処理は、
リモートメンテナンス要求を受けて設定したリモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、確立した前記ＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する様、前記ＶＰＮゲートウェイに対して行い、前記インターネットゲートウェイ端末に対して、リモートメンテナンス対象の内線端末名を通知し、その後、前記第３判断にリターンする一連の処理であり、
前記ＶＰＮ終了処理は、
ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に対して送信して、前記ＶＰＮゲートウェイに、リモートメンテナンス実施要求の際に設定した前記ＶＰＮトンネルの解除させ、当該ＶＰＮゲートウェイと当該インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了させる一連の処理である、
ことを特徴とする請求項１８に記載のリモートメンテナンス実施プログラム。
【請求項２０】請求項１３、１４、１５、１６、１７、１８又は１９に記載のリモートメンテナンス実施プログラムによる一連の手続を実録した、
ことを特徴とするリモートメンテナンス実施プログラムを記録した記録媒体。
【請求項２１】インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行う実施方法であって、
ＶＰＮを構築する前に、前記インターネットゲートウェイ端末からのＶＰＮ構築要求を受けた前記保守センタが、その配下の複数のＶＰＮゲートウェイからＶＰＮの空きリソースのあるＶＰＮゲートウェイを動的に選択して、当該選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを当該インターネットゲートウェイ端末に通知し、当該インターネットゲートウェイ端末は当該通知されたグローバルＩＰアドレスを当該ＶＰＮの対向ホストとして設定を行うことにより、前記リモートメンテナンスを実施する、
ことを特徴とするリモートメンテナンス実施方法。
【請求項２２】インターネットに接続された複数のイン

ターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムであって、
前記インターネットゲートウェイ端末からＶＰＮ構築の要求を受けると、その配下の複数のＶＰＮゲートウェイからＶＰＮの空きリソースのあるＶＰＮゲートウェイを動的に選択して、当該選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを、当該要求をなしたインターネットゲートウェイ端末に通知する前記保守センタと、
当該保守センタに対して前記ＶＰＮ構築の要求を行うと共に、当該要求に対する当該保守センタから前記通知された前記選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを、当該ＶＰＮの対向ホストとして設定する前記インターネットゲートウェイ端末と、
を具備する、
ことを特徴とするリモートメンテナンス実施システム。
【請求項２３】インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、
前記内線端末からのリモートメンテナンス要求の登録又はインターネットゲートウェイ端末管理者による前記インターネットゲートウェイ端末本体のボタン操作の何れかにより、ＶＰＮゲートウェイアドレスを要求するＶＰＮゲートウェイアドレス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、
前記保守センタに対して前記ＶＰＮゲートウェイアドレスの要求を行うと共に、
当該保守センタから当該要求に対するＶＰＮゲートウェイアドレス要求レスポンスを受信すると、当該ＶＰＮゲートウェイアドレス要求レスポンスとして受信したＶＰＮゲートウェイグローバルＩＰアドレスを、ＶＰＮの対向ホストとして、自己のルータ部に設定して、前記リモートメンテナンス要求の処理を行う、以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項２４】インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該保守センタにて用いられるプログラムであって、
前記インターネットゲートウェイ端末からのＶＰＮゲートウェイアドレス要求に伴う前記保守センタ内の処理であるＶＰＮゲートウェイアドレス要求処理を当該保守センタに行わせる前記プログラムの実行により、
前記インターネットゲートウェイ端末から前記ＶＰＮゲートウェイアドレス要求を受信すると、自己の支配下の複数のＶＰＮゲートウェイからＶＰＮ空きリソースのあるＶＰＮゲートウェイを動的に選択し、そのＶＰＮゲートウェイのグローバルＩＰアドレスを、当該ＶＰＮゲートウェイアドレス要求をなしたインターネットゲートウェイ端末に通知する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項２５】請求項２３又は２４に記載のリモートメンテナンス実施プログラムによる一連の手続を実録した、
ことを特徴とするリモートメンテナンス実施プログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネットに接続された保守センタからインターネットゲートウェイ端末自体及びそのインターネットゲートウェイ端末配下のローカルネットワークに接続されたパソコン等の内線端末をインターネット経由でＶＰＮを利用してリモートメンテナンスを行うリモートメンテナンス実施方法、その実施に直接使用するリモートメンテナンスシステム、プログラム及び同記録媒体に関するものである。
【０００２】
【従来の技術】従来、インターネットに接続された保守センタからインターネットゲートウェイ端末（以下、情流ＧＷ端末）自体及びその情流ＧＷ端末に接続されたローカルネットワーク上のパソコン（以下、内線端末）をインターネット経由でＶＰＮを利用してリモートメンテナンスを行うリモートメンテナンス実施方法（以下、ＶＰＮリモートメンテナンスと呼ぶ）として、特願平２０００－０００４９６で提案されている方法がある。
【０００３】しかし、特願平２０００－０００４９６の方法で提案されているＶＰＮリモートメンテナンスでは、複数の情流ＧＷ端末に対して同時にリモートメンテ

ナンスを行う際、対象となる情流ＧＷ端末配下のローカルネットワークアドレスが重複している場合、保守センタからＶＰＮ経由でリモートメンテナンス対象の情流ＧＷ端末及びその配下の内線端末にパケットを送るとき、対象ローカルＩＰアドレスがバッティングするため、保守センタ側のＶＰＮゲートウェイでは、どちらのローカルネットワークへパケットを送出してよいか判断できず、同時に同じローカルネットワークアドレスを持つ複数の情流ＧＷへのメンテナンスを行うことが不可能であった。

【０００４】そこで、保守センタのローカルネットワーク内から、配下に同じローカルネットワークアドレスを持つ複数の情流ＧＷへ同時にメンテナンスを行う方法として、インターネット側から各々の情流ＧＷの内部ネットワークを見たときにそのローカルネットワークアドレスがユニークになるようにする手法が考えられる。

【０００５】具体的には、情流ＧＷの内部に、保守センタ側とＶＰＮ通信するための仮のローカルネットワークアドレス（以下、ＶＰＮＮＡＴ用ＩＰアドレス）とローカルネットワークアドレスを固定して結びつける処理部（以下、ＮＡＴＢＯＸ）を設けるという手法であり、図３２を元に動作を説明する。

【０００６】図３２において、クライアントＰＣ（ａ）からサーバＰＣ（ｂ）へＶＰＮＮＡＴ経由でＩＰ通信を行う場合の、パケットのアドレスの変化を示すために、まず、各ノードの接続形態を説明する。クライアントＰＣ（ａ）は、プライベートネットワーク（ｃ）に接続されており192.168.2.103のプライベートＩＰアドレスを持つ。ＶＰＮゲートウェイ（ｄ）は、プライベートネットワーク（ｃ）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして211.0.0.1を持つ。

【０００７】ＶＰＮルータ（ｆ）は、プライベートネットワーク（ｇ）に接続されており、インターネット側のグローバルＩＰアドレスとして210.0.0.1を持つ。サーバＰＣ（ｂ）はプライベートネットワーク（ｃ）に接続されており、192.168.1.1～192.168.1.254のプライベートＩＰアドレスを持つ。

【０００８】また、ＶＰＮゲートウェイ（ｄ）と情流ＧＷ（以下、ＶＰＮルータとも呼ぶ）は、ＶＰＮのトンネル（ｈ）を構築している。ＶＰＮゲートウェイ（ｄ）ではＶＰＮルータ（ｂ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットとして10.0.0.0/24が設定されており、ＶＰＮルータ（ｂ）では、ＶＰＮゲートウェイ（ｄ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットとして192.168.2.0/24が設定されている。

【０００９】また、ＮＡＴＢＯＸ（ｆ１０）は、インターネット（ｅ）側にＶＰＮＮＡＴ用ＩＰアドレスとして10.0.0.1～10.0.0.254のアドレスを持ち、10.0.0.1と192.168.1.1、10.0.0.2と192.168.1.2、…（省略）、…、10.0.0.254と192.168.1.254で静的ＮＡＴが設定されている。

【００１０】ここで、192.168.1.1のサーバＰＣ（ｂ）について着目すると、ＮＡＴＢＯＸ（ｆ１０）のプライベートネットワーク（ｇ）側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.0.1に書き換えられてＮＡＴＢＯＸ（ｆ１０）のインターネット側へ送出され、ＮＡＴＢＯＸ（ｆ１０）のインターネット（ｅ）側から送信先10.0.0.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてＮＡＴＢＯＸ（ｆ１０）のプライベートネットワーク（ｃ）側に送出される。

【００１１】以下、クライアントＰＣ（ａ）とサーバＰＣ（ｂ）間で通信を行う際のパケットのアドレス変化を示す。ここで、クライアントＰＣ（ａ）からサーバＰＣ（ｂ）宛てのオリジナルパケットは、「送信元192.168.2.103：送信先10.0.0.1」で送出され、ＶＰＮゲートウェイ（ｄ）に到着する。

【００１２】ＶＰＮゲートウェイ（ｄ）は、10.0.0.1のパケットを受信したのでＶＰＮルータ（ｆ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットと判断し、「送信元211.0.0.1：送信先210.0.0.1」の新ＩＰヘッダを付加し、カプセル化を行う。オリジナルパケットは暗号化されてデータ部に入る。このパケットは、ＶＰＮトンネルを経由してＶＰＮルータのＶＰＮ処理部（ｆ１１）に到達する。

【００１３】ＶＰＮルータのＶＰＮ処理部（ｆ１１）では、オリジナルパケットが復号化され、「送信元192.168.2.103：送信先10.0.0.1」としてＮＡＴＢＯＸ（ｆ１０）に送出する。ＮＡＴＢＯＸ（ｆ１０）では、外側10.0.0.1と内側192.168.1.1で静的ＮＡＴが設定されており、送信先アドレスが10.0.0.1にマッチするので、アドレス変換が行われ、「送信元192.168.2.103：送信先192.168.1.1」となり、プライベートネットワーク（ｃ）のネットワークに送出される。したがって、このパケットは、サーバＰＣ（ｂ）に到着することができる。

【００１４】また、サーバＰＣ（ｂ）からクライアントＰＣ（ａ）へのレスポンスオリジナルパケットは、「送信元192.168.1.1：送信先192.168.2.103」で送出され、ＶＰＮルータ（ｆ）に到着する。ＶＰＮルータ（ｆ）では、192.168.2.0/24のパケットを受信したのでＶＰＮゲートウェイ（ｄ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットと判断し、まずＮＡＴＢＯＸ（ｆ１０）にパケットが送られる。

【００１５】ＮＡＴＢＯＸ（ｆ１０）では、外側10.0.0.1と内側192.168.1.1で静的ＮＡＴが設定されており、送信元アドレスが192.168.1.1にマッチするので、アドレス変換が行われ「送信元10.0.0.1：送信先192.168.2.103」となり、ＶＰＮ処理部（ｂ１１）へ送られる。

【００１６】ＶＰＮ処理部（ｆ１１）では「送信元210.

0.0.1：送信先211.0.0.1」となり新ＩＰヘッダを付加し、カプセル化を行う。レスポンスオリジナルパケットは暗号化されてデータ部に入る。このパケットは、ＶＰＮトンネル（ｈ）を経由してＶＰＮゲートウェイ（ｄ）に到達する。ＶＰＮゲートウェイ（ｄ）では、レスポンスオリジナルパケットが復号化され、「送信元10.0.0.1：送信先192.168.2.103」となり、プライベートネットワーク（ｃ）のネットワークに送出される。したがって、このパケットは、クライアントＰＣ（ａ）に到着することができる。

【００１７】以上、保守センタから情流ＧＷ（ｆ）１台で配下のローカルネットワークが１つの場合について保守センタのプライベートネットワーク（ｇ）と情流ＧＷ（ｆ）配下のプライベートネットワーク（ｃ）を静的ＶＰＮＮＡＴ機能を適用して通信を行った場合の動作概要について説明した。なお、図中（ｆ１）はＮＡＴＢＯＸ（ｆ１０）とＶＰＮ処理部（ｆ１１）で構成されるルータ部である。

【００１８】次に、保守センタから情流ＧＷ（ｆ’）（ｆ″）２台の配下のプライベートネットワーク（ｇ’）（ｇ″）が２つあり、そのプライベートネットワークアドレスが重複している場合について、保守センタのプライベートネットワーク（ｃ）から各々の情流ＧＷ（ｆ’）（ｆ″）配下のプライベートネットワーク（ｇ’）（ｇ″）に対して静的ＶＰＮＮＡＴ機能を適用して通信を行う場合の動作概要について説明する。

【００１９】図３３に情流ＧＷ（ｆ’）（ｆ″）２台の配下のプライベートネットワークネットワークアドレスが同じケースにおいて、静的ＶＰＮＮＡＴ機能を用いて保守センタから２つの情流ＧＷ（ｆ’）（ｆ″）配下のアドレスのサーバＰＣ（ｂ１）～（ｂ４）に同時にアクセスする方法を示す。

【００２０】ここで、クライアントＰＣ（ａ）からサーバＰＣ（ｂ１）～（ｂ４）へＶＰＮＮＡＴ経由でＩＰ通信を行う場合の、パケットのアドレスの変化を示すために、まず、各ノードの接続形態を説明する。クライアントＰＣ（ａ）は、プライベートネットワーク（ｇ’）（ｇ″）に接続されており192.168.2.103のプライベートＩＰアドレスを持つ。ＶＰＮゲートウェイ（ｄ）は、プライベートネットワーク（ｃ）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして211.0.0.1を持つ。

【００２１】ＶＰＮルータ（ｆ’）は、プライベートネットワーク（ｇ’）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして210.0.0.1を持つ。サーバＰＣ（ｂ１）（ｂ２）はＶＰＮルータ（ｆ’）の内部ローカルネットワーク192.168.1.0/24に接続されており、192.168.1.1～192.168.1.254のプライベートＩＰアドレスを持つ。また、ＶＰＮゲートウェイ（ｄ）とＶＰＮルータ（ｆ’）は、ＶＰＮのトンネル（ｈ’）を構築している。

【００２２】ＶＰＮゲートウェイ（ｄ）ではＶＰＮルータ（ｆ’）へのＶＰＮトンネル（ｈ’）に対してのＶＰＮ対象パケットとして10.0.0.0/24が設定されており、ＶＰＮルータ（ｆ’）では、ＶＰＮゲートウェイ(ｄ)へのＶＰＮトンネル（ｈ’）に対してのＶＰＮ対象パケットとして192.168.2.0/24が設定されている。

【００２３】また、ＮＡＴＢＯＸ（ｆ１０’）は、インターネット（ｅ）側にＶＰＮＮＡＴ用ＩＰアドレスとして10.0.0.1～10.0.0.254のアドレスを持ち、10.0.0.1と192.168.1.1、10.0.0.2と192.168.1.2、…、（省略）、…、10.0.0.254と192.168.1.254で静的ＮＡＴが設定されている。

【００２４】ここで、192.168.1.1のサーバＰＣ（ｂ１）（ｂ２）について着目すると、ＮＡＴＢＯＸ（ｆ１０）のプライベートネットワーク（ｇ’）側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.0.1に書き換えられてＮＡＴＢＯＸ（ｆ１０’）のインターネット側へ送出され、ＮＡＴＢＯＸ（ｆ１０’）のインターネット（ｅ）側から送信先10.0.0.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてＮＡＴＢＯＸ（ｆ’）のプライベートネットワーク側に送出される。

【００２５】ＶＰＮルータ（ｆ″）は、プライベートネットワーク（ｇ″）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして210.0.1.1を持つ。サーバＰＣ（ｂ３）（ｂ４）はＶＰＮルータ（ｆ″）の内部ローカルネットワーク192.168.1.0/24に接続されており、192.168.1.1～192.168.1.254のプライベートＩＰアドレスを持つ。

【００２６】また、ＶＰＮゲートウェイ（ｄ）とＶＰＮルータ（ｆ″）は、ＶＰＮのトンネル（ｈ″）を構築している。ＶＰＮゲートウェイ（ｄ）ではＶＰＮルータ（ｆ″）へのＶＰＮトンネル（ｈ″）に対してのＶＰＮ対象パケットとして10.0.1.0/24が設定されており、ＶＰＮルータ（ｆ″）では、ＶＰＮゲートウェイ（ｄ）へのＶＰＮトンネル（ｈ″）に対してのＶＰＮ対象パケットとして192.168.2, 0/24が設定されている。

【００２７】また、ＮＡＴＢＯＸ（ｆ１０″）は、インターネット（ｅ）側にＶＰＮＮＡＴ用ＩＰアドレスとして10.0.1.1～10.0.1.254のアドレスを持ち、10.0.1.1と192.168.1.1、10.0.1.2と192.168.1.2、…、（省略）、…、10.0.1.254と192.168.1.254で静的ＮＡＴが設定されている。

【００２８】ここで、192.168.1.1のサーバＰＣＢについて着目すると、ＮＡＴＢＯＸ（ｆ″）のプライベートネットワーク（ｇ″）側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.1.1に書き換えられてＮＡＴＢＯＸ（ｆ″）のインターネット（ｅ）側へ送出され、ＮＡＴＢＯＸ（ｆ″）のイン

ターネット（ｅ）側から送信先10.0.1.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてＮＡＴＢＯＸ（ｆ″）のプライベートネットワーク（ｇ″）側に送出される。

【００２９】以上、保守センタから情流ＧＷ（ｆ′）（ｆ″）２台の配下のプライベートネットワーク（ｇ′）（ｇ″）が２つあり、そのプライベートネットワークアドレスが重複している場合について、保守センタのプライベートネットワーク（ｃ）から各々の情流ＧＷ（ｆ′）（ｆ″）配下のプライベートネットワーク（ｇ′）（ｇ″）に対して静的VＰＮＮＡＴ機能を適用して通信を行う場合の動作概要について説明した。

【００３０】言うまでもないが、前記示した「情流ＧＷ２台の配下のプライベートネットワークが２つあり、そのプライベートネットワークアドレスが重複している場合」の動作は、「情流ＧＷＮ（Ｎは任意の自然数）台の配下のプライベートネットワークがＮ個あり、そのプライベートネットワークアドレスが重複している場合」にも適用できる。

【００３１】従って、図３３に示す方法で、静的ＶＰＮＮＡＴを構築した上で保守センタからアクセスすることにより、複数の情流ＧＷ端末（ＶＰＮルータ）に対して同時にリモートメンテナンスを行う際、対象となる情流ＧＷ端末配下のプライベートネットワークアドレスが重複している場合でも、保守センタからＶＰＮ経由でリモートメンテナンス対象の情流ＧＷ端末及びその配下の内線端末（サーバＰＣ）にパケットを送るとき、対象プライベートＩＰアドレスを静的ＶＰＮＮＡＴで割り付けたＮＡＴＢＯＸのインターネット側のアドレス向けに送出することにより、保守センタ側のＶＰＮゲートウェイでは、どちらのプライベートネットワークへパケットを送出してよいか判断でき、同時に同じプライベートネットワークアドレスを持つ複数の情流ＧＷ端末へのメンテナンスを行うことが可能となる。以下、これを「静的ＶＰＮＮＡＴ方式」と呼ぶことにする。

【００３２】また、特願平２０００－０００４９６にて提案されているＶＰＮリモートメンテナンスでは、保守センタのＶＰＮゲートウェイのグローバルＩＰアドレスを情流ＧＷ端末が事前に知っていることを必須とし、その対応策とて、事前に情流ＧＷ端末にＶＰＮゲートウェイのグローバルＩＰアドレスを埋め込んで出荷するという方法が採られていた。

【００３３】

【発明が解決しようとする課題】しかし、前記説明した「静的ＶＰＮＮＡＴ」方式により保守センタのプライベートネットワークから情流ＧＷ端末配下の全てのプライベートネットワークに対してアクセスする場合は、情流ＧＷ端末とＶＰＮゲートウェイ間でＶＰＮを構築する時点で、情流ＧＷ端末においてＶＰＮＮＡＴ用ＩＰアドレスとプライベートネットワークの実ローカルＩＰアドレスを事前に静的ＶＰＮＮＡＴで割り付けておく必要があった。

【００３４】この場合、保守センタ側がユニークに管理するＶＰＮＮＡＴ用ＩＰアドレスリソース（プライベートＩＰアドレス）を保守対象の情流ＧＷ端末配下のプライベートネットワークの端末台数分だけ事前に割り当てる必要があり、実際にメンテナンスを行う対象端末数に対して、非常に膨大な数のＶＰＮＮＡＴ用ＩＰアドレスリソースを必要とした。すなわち静的ＶＰＮＮＡＴ方式では、同クラスのプライベートＩＰアドレスを使った場合、最大約１６７０万台の情流ＧＷ端末配下の内線端末だけがリモートメンテナンス対象端末であった。

【００３５】例えば、同クラスのプライベートアドレスをＶＰＮＮＡＴ用ＩＰアドレスリソースとして利用し、情流ＧＷ端末配下のプライベートネットワークのサブネットマスクが全て２４ビットだった場合は最大約６万５千加入情流ＧＷ端末配下のプライベートネットワークのサブネットマスクが全て１６ビットだった場合は最大約２５６加入の情流ＧＷ端末配下の端末しかメンテナンス対象とできないという制約事項があった。

【００３６】また、静的ＶＰＮＮＡＴ方式を使って、特願平２０００－０００４９６の方法で提案されているＶＰＮリモートメンテナンスを行う場合は、リモートメンテナンス要求をあげた情流ＧＷ端末配下の全ての内線端末リソースに保守センタからアクセスが可能となってしまうという問題点があった。

【００３７】また、ＶＰＮリモートメンテナンスの設置通知数が増大し、ＶＰＮリモートメンテナンスサービスの同時利用者がＶＰＮゲートウェイの許容ＶＰＮセッション数を超える場合、保守センタ側でＶＰＮゲートウェイを増設して設置する必要があり、その場合、ＶＰＮゲートウェイのグローバルＩＰアドレスを端末に設定させる手段が存在しなかった。また、保守センタのＶＰＮゲートウェイアドレスを何らかの手段でインターネットゲートウェイ管理者に通知し、手動でＶＰＮゲートウェイアドレスを設定させる方法は、リモートメンテナンスの際に人手が伴うので、ＶＰＮリモートメンテナンスには適用できないという問題点があった。

【００３８】ここにおいて、本発明の解決すべき主要な目的は次の通りである。

【００３９】本発明の第１の目的は、保守センタからインターネットのＶＰＮ経由で、配下のプライベート（ローカル）ネットワークアドレスの重複を許容した複数の情流ＧＷ端末及びその内線端末を同時にリモートメンテナンスする際、リモートメンテナンス対象の情流ＧＷ端末及び内線端末数の制限を、保守センタ側で管理するＩＰアドレスリソースの上限まで許容し、可能な限り多数の情流ＧＷ端末及びその配下の内線端末のリモートメンテナンスを同時に行うことを可能とするリモートメンテナンス実施方法、システム、プログラム及び記録媒体を

提供せんとするものである。

【００４０】本発明の第２の目的は、保守センタ側がユニークに管理するＶＰＮＮＡＴ要ＩＰアドレスリソースを保守対象の情流ＧＷ端末配下のプライベートネットワークの端末台数分だけ事前に割り当てる必要のないリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４１】本発明の第３の目的は、ＶＰＮリモートメンテナンスを行う場合に、リモートメンテナンス要求をあげた情流ＧＷ端末配下のすべての内線端末リソースに保守センタからのアクセスが起こらないようにしたリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４２】本発明の第４の目的は、ＶＰＮリモートメンテナンスの設置通知数が増大しＶＰＮリモートメンテナンスの同時利用者が、ＶＰＮゲートウェイの許容ＶＰＮセッション数を超える場合、保守センタ側でＶＰＮゲートウェイを増設して設置する必要があるが、その場合にＶＰＮゲートウェイのグローバルＩＰアドレスを端末に設定するようにしたリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４３】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【００４４】

【課題を解決するための手段】本発明方法は、上記課題の解決に当たり、①各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行う実施方法であり、当該インターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして当該保守センタから付与及び解放を行うことで実施した、特徴的構成手法、②インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行う実施方法であって、ＶＰＮを構築する前に、前記インターネットゲートウェイ端末からのＶＰＮ構築要求を受けた前記保守センタが、その配下の複数のＶＰＮゲートウェイからＶＰＮの空きリソースのあるＶＰＮゲートウェイを動的に選択して、当該選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを当該インターネットゲートウェイ端末に通知し、当該インターネットゲートウェイ端末は当該通知されたグローバルＩＰアドレスを当該ＶＰＮの対向ホストとして設定を行うことにより、前記リモートメンテナンスを実施する、特徴的構成手法を講じる。

【００４５】本発明システムは、上記課題の解決に当たり、①各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行う実施システムであり、当該インターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴ手段を設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして当該保守センタから付与及び解放を行える機能構成にシステム構築した、特徴的構成手段、②インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムであって、前記インターネットゲートウェイ端末からＶＰＮ構築の要求を受けると、自己の配下の複数のＶＰＮゲートウェイからＶＰＮの空きリソースのあるＶＰＮゲートウェイを動的に選択して、当該選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを、当該要求をなしたインターネットゲートウェイ端末に通知する前記保守センタと、当該保守センタに対して前記ＶＰＮ構築の要求を行うと共に、当該要求に対する当該保守センタから前記通知された前記選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを、当該ＶＰＮの対向ホストとして設定する前記インターネットゲートウェイ端末とを具備する、特徴的構成手段を講じる。

【００４６】本発明プログラムは、上記課題の解決に当たり、①各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層に

おいてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該インターネットゲートウェイ端末、当該保守センタにて用いられるプログラムで、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして当該保守センタから付与、解放を行う各種の処理手順を実行した、特徴的構成手順、②インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにて、当該インターネットゲートウェイ端末、当該保守センタにて用いられるプログラムで、当該インターネットゲートウェイ端末がＶＰＮＧＷアドレス要求を行い、当該ＶＰＮＧＷアドレス要求に応じて当該保守サーバから通知されたＶＰＮゲートウェイアドレスを、ＶＰＮの対向ホストとして、自己のルータ部に設定する処理手順、また、当該ＶＰＮＧＷアドレス要求を受信すると、自己の支配下の複数のＶＰＮゲートウェイからＶＰＮ空きリソースのあるＶＰＮゲートウェイを動的に選択し、そのＶＰＮゲートウェイのグローバルＩＰアドレスを、当該ＶＰＮゲートウェイアドレス要求をなしたインターネットゲートウェイ端末に通知する処理手順を実行した、特徴的構成手順、を講じる。

【００４７】本発明記録媒体は、上記課題の解決に当たり、本発明プログラムにより一連の完結手続を実録した、特徴的構成手続を講じる。

【００４８】更に具体的に詳説すると、当該課題の解決では、本発明が次に列挙する新規な各特徴的構成手法、手段、手順又は手続を講じることにより、上記目的を達成する様になされる。

【００４９】本発明方法の第１の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行う実施方法であって、前記それぞれのインターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタの保守サーバから付与及び解放を行うことにより前記リモートメンテナンスを実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５０】本発明方法の第２の特徴は、上記本発明方法の第１の特徴における前記実施方法における前記リモートメンテナンスの要求が、当該要求を行う前記インターネットゲートウェイ端末が、リモートメンテナンス対象である内線端末名及び当該インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知すると、当該通知を受けた当該保守サーバが、当該通知したリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該通知をしてきたインターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとしてレスポンスすると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において設置通知の際に共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を自己のＶＰＮゲートウェイに設定させ、当該ＶＰＮゲートウェイに対してＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを前記確立したＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行い、前記レスポンスを受けたインターネットゲートウェイ端末が、受けた前記内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと前記ＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとし自己のルータ部に対して設定を行う、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【００５１】本発明方法の第３の特徴は、上記本発明方法の第２の特徴における前記リモートメンテナンスの実施が、前記リモートメンテナンス対象である前記内線端末に対して、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、前記保守センタから行われてなる、リモートメンテナンス実施方法の構成採用にある。

【００５２】本発明方法の第４の特徴は、上記本発明方法の第２又は第３の特徴における前記リモートメンテナンスの終了が、先ず、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信し、次に、当該送信を受けたサーバ部において、当該リモートメンテナンス終了コマンドに係る処理を行い、リモートメンテナンス終了レスポンスを送信し、その後、当該リモートメンテナンス終了レスポンスを受信した保守サーバにて、該当内線端末に対するメンテナンスが全て終了したかの第１判断を行い、当該第１判断にて肯定の場合には当該終了した内線端末は前記インターネットゲートウェイ端末の前記サーバ部、前記ルータ部の何れかであるかの第２判断を行う一方、否定の場合には判断処理を終了し、当該第２判断

にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行し、他方肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行するとともに否定の場合には当該判断処理を終了する、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【００５３】本発明方法の第５の特徴は、上記本発明方法の第４の特徴における前記ＶＰＮＮＡＴ解放処理が、先ず、前記保守サーバが、前記リモートメンテナンスの要求の際に設定した前記リモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、前記確立したＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する一方で、前記インターネットゲートウェイ端末に対して当該リモートメンテナンス対象の内線端末名を通知した後に、当該通知を受けたインターネットゲートウェイ端末が、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得して、それに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放し、引続き、前記保守サーバが、前記第３判断を行いその判断結果に従う、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【００５４】本発明方法の第６の特徴は、上記本発明方法の第４又は第５の特徴における前記ＶＰＮ終了処理が、前記保守サーバが、ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に通知して、当該通知を受けたインターネットゲートウェイ端末が、当該ＶＰＮ終了コマンドに対する返答を当該保守サーバにＶＰＮ終了レスポンスとして送信し、前記保守サーバが、前記ＶＰＮゲートウェイに、前記リモートメンテナンスの要求に際に設定した前記ＶＰＮトンネルを解除させ、当該ＶＰＮゲートウェイと前記インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５５】本発明方法の第７の特徴は、上記本発明方法の第２、第３、第４、第５又は第６の特徴における前記設置通知が、新たに設置された前記インターネットゲートウェイ端末の前記サーバ部から、当該設置について前記保守サーバに設置通知コマンドを通知し、当該設置通知コマンドを受けた当該保守サーバにより、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスし、当該レスポンスを受信した前記インターネットゲートウェイ端末は、ＩＰｓｅｃの認証鍵を自己の前記ルータ部に対して設定する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５６】本発明方法の第８の特徴は、上記本発明方法の第２、第３、第４、第５、第６又は第７の特徴における前記実施方法が、前記リモートメンテナンスの要求、前記設定通知の何れか一方において、前記インターネットゲートウェイ端末の前記サーバ部及び前記ルータ部へのＶＰＮＮＡＴ設定処理を実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５７】本発明方法の第９の特徴は、上記本発明方法の第２、第３、第４、第５、第６、第７又は第８の特徴における前記実施方法が、前記インターネットゲートウェイ端末に故障発生を検知した場合には、先ず、当該インターネットゲートウェイ端末が、故障通知コマンドとして故障に係る情報を前記保守サーバに送信し、次に、前記保守サーバが前記故障通知コマンドを受信すると当該故障に係る情報を処理して、当該故障通知コマンドを送信した前記インターネットゲートウェイ端末に故障通知レスポンスとして送信し、更に、当該故障通知レスポンスを受信した当該インターネットゲートウェイ端末が前記リモートメンテナンスの要求に移行する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５８】本発明方法の第１０の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行う実施方法であって、ＶＰＮを構築する前に、前記インターネットゲートウェイ端末からのＶＰＮ構築要求を受けた前記保守センタが、その配下の複数のＶＰＮゲートウェイからＶＰＮの空きリソースのあるＶＰＮゲートウェイを動的に選択して、当該選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを当該インターネットゲートウェイ端末に通知し、当該インターネットゲートウェイ端末は当該通知されたグローバルＩＰアドレスを当該ＶＰＮの対向ホストとして設定を行うことにより、前記リモートメンテナンスを実施してなるリモートメンテナンス実施方法の構成採用にある。（請求項２１に対応）

【００５９】本発明システムの第１の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテ

ナンスを行うシステムであって、前記インターネットゲートウェイ端末におけるルータ部内にそのローカルネットワークとＶＰＮ処理部との間にＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタから付与及び解放を行う機能構成にシステム構築してなるリモートメンテナンス実施システムの構成採用にある。

【００６０】本発明システムの第２の特徴は、上記本発明システムの第１の特徴における前記保守センタが、前記インターネットゲートウェイ端末からリモートメンテナンス対象の内線端末名の通知を受けて当該リモートメンテナンス対象の内線端末名に対応するＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルアドレスの付与を行う保守サーバと、前記リモートメンテナンスを行うリモートメンテナンス装置と、当該リモートメンテナンス装置からの、当該リモートメンテナンス対象の内線端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスへアクセスを経由するＶＰＮゲートウェイとを、保守センタローカルネットワークにてネットワーク構築してなるリモートメンテナンス実施システムの構成採用にある。

【００６１】本発明システムの第３の特徴は、上記本発明システムの第１又は第２の特徴における前記インターネットゲートウェイ端末が、前記保守センタにリモートメンテナンス対象の内線端末名を通知するサーバ部と、当該通知したことにより当該保守センタから付与されたＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルＩＰアドレスと当該リモートメンテナンス対象の内線端末名のＩＰアドレスを割りつけるＶＰＮＮＡＴ及び当該保守センタの前記ＶＰＮゲートウェイとＶＰＮトンネルを確立するＶＰＮ処理部のルータ部とで構成して、前記ＶＰＮゲートウェイを介した、リモートメンテナンス対象端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスへのアクセスにより、前記リモートメンテナンスを行うリモートメンテナンス装置からの、前記内線端末へのパケット転送を可能ならしめる機能を構築してなるリモートメンテナンス実施システムの構成採用にある。

【００６２】本発明システムの第４の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムであって、前記インターネットゲートウェイ端末からＶＰＮ構築の要求を受けると、その配下の複数のＶＰＮゲートウェイからＶＰＮの空きリソースのあるＶＰＮゲートウェイを動的に選択して、当該選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを、当該要求をなしたインターネットゲートウェイ端末に通知する前記保守センタと、当該保守センタに対して前記ＶＰＮ構築の要求を行うと共に、当該要求に対する当該保守センタから前記通知された前記選択されたＶＰＮゲートウェイのグローバルＩＰアドレスを、当該ＶＰＮの対向ホストとして設定する前記インターネットゲートウェイ端末とを具備してなるリモートメンテナンス実施システムの構成採用にある。

（請求項２２に対応）

【００６３】本発明プログラムの第１の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末で用いられるプログラムであって、当該インターネットゲートウェイ端末が設置された後に、リモートメンテナンスサービスを利用する場合に、前記保守センタに対して設置した旨を通知する設置通知処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、前記設置について前記保守センタの保守サーバに設置通知コマンドを通知した後に、当該保守サーバからの当該設置通知コマンドに対するレスポンスを受信すると当該レスポンスとして受けたＩＰｓｅｃの認証鍵を自己のルータ部に対して設定する、一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６４】本発明プログラムの第２の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、当該インターネットゲートウェイ端末への、前記内部端末からのＷＥＢアクセス、当該インターネットゲートウェイ端末の操作者によるボタン操作の何れかにより、リモートメンテナンスを要求するリモートメンテナンス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、リモートメンテナンス対象である前記内線端末名及び前記インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知した後に、前記リモートメンテナンス要求コマンドに対するレスポンスを受けて、当該レスポンスとして受けた、

内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと当該レスポンスとして受けたＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとして設定させる、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６５】本発明プログラムの第３の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、前記保守センタより行われる前記リモートメンテナンスの作業が終了した旨の通知に係るリモートメンテナンス終了処理を、当該通知を受けた前記インフェースゲートウェイ端末に行わせる前記プログラムの実行により、前記保守センタからのリモートメンテナンス終了コマンドの受信を契機に、当該リモートメンテナンス終了コマンドに関する処理を行い、リモートメンテナンス終了レスポンスを送信して、前記保守センタからＶＰＮ解放コマンドとしてリモートメンテナンス対象の内線端末名の通知を受けた場合には、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得し、取得した実ローカルＩＰアドレスに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６６】本発明プログラムの第４の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記リモートメンテナンスの要求に対応するリモートメンテナンス要求処理を前記保守サーバに行わせる前記プログラムの実行により、前記要求を受けて、前記リモートメンテナンスの要求に係るリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該要求を行った前記インターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとして送信すると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を、自己のＶＰＮゲートウェイに指示し、自己の当該ＶＰＮゲートウェイに対して、ＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを、当該指示により確立されるＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行う、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６７】本発明プログラムの第５の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該保守センタにて用いられるプログラムであって、新たに設置された前記インターネットゲートウェイ端末からの設置通知コマンドを処理する設定通知コマンド処理を前記保守センタに行わせる前記プログラムの実行により、前記設置通知コマンドに応じて、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスする、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６８】本発明プログラムの第６の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記保守センタにおける終了ボタンが押されたことを契機に、前記リモートメンテナンスの作業が終了したことを通知するリモートメンテナンス終了処理を、前記保守サーバに行わせる前記プログラムの実行により、ＶＰＮＮＡＴ用ローカルＩＰアドレスで確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信した後に、当該リモートメンテナンス終了のレスポンスを受信すると、該当内線端末に対するメンテナンスが全て終了したかのを第１判断を行い、当該第１判断にて肯定の場合には当該終了した前記内線端末は前記インターネットゲートウェイ端末の前記サーバ部かルータ部かの何れかであるかの第２判断を行う一方、否定の場合にはこのプログラムを終了し、

当該第２判断にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行する一方、肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行する一方、否定の場合にはこのプログラムを終了する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６９】本発明プログラムの第７の特徴は、上記本発明プログラムの第６の特徴における前記ＶＰＮＮＡＴ解放処理が、リモートメンテナンス要求を受けて設定したリモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、確立した前記ＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する様、前記ＶＰＮゲートウェイに対して行い、前記インターネットゲートウェイ端末に対して、リモートメンテナンス対象の内線端末名を通知し、その後、前記第３判断にリターンする一連の処理であり、前記ＶＰＮ終了処理が、ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に対して送信して、前記ＶＰＮゲートウェイに、リモートメンテナンス実施要求の際に設定した前記ＶＰＮトンネルの解除させ、当該ＶＰＮゲートウェイと当該インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了させる一連の処理であるリモートメンテナンス実施プログラムの構成採用にある。

【００７０】本発明プログラムの第８の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、前記内線端末からのリモートメンテナンス要求の登録又はインターネットゲートウェイ端末管理者による前記インターネットゲートウェイ端末本体のボタン操作の何れかにより、ＶＰＮゲートウェイアドレスを要求するＶＰＮゲートウェイアドレス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、前記保守センタに対して前記ＶＰＮゲートウェイアドレスの要求を行うと共に、当該保守センタから当該要求に対するＶＰＮゲートウェイアドレス要求レスポンスを受信すると、当該ＶＰＮゲートウェイアドレス要求レスポンスとして受信したＶＰＮゲートウェイグローバルＩＰアドレスを、ＶＰＮの対向ホストとして、自己のルータ部に設定して、前記リモートメンテナンス要求の処理を行う、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。（請求項２３に対応）

【００７１】本発明プログラムの第９の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにＩＰ接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該保守センタにて用いられるプログラムであって、前記インターネットゲートウェイ端末からのＶＰＮゲートウェイアドレス要求に伴う前記保守センタ内の処理であるＶＰＮゲートウェイアドレス要求処理を当該保守センタに行わせる前記プログラムの実行により、前記インターネットゲートウェイ端末から前記ＶＰＮゲートウェイアドレス要求を受信すると、自己の支配下の複数のＶＰＮゲートウェイからＶＰＮ空きリソースのあるＶＰＮゲートウェイを動的に選択し、そのＶＰＮゲートウェイのグローバルＩＰアドレスを、当該ＶＰＮゲートウェイアドレス要求をなしたインターネットゲートウェイ端末に通知する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。（請求項２４に対応）

【００７２】本発明記録媒体の第１の特徴は、上記本発明プログラムの第１、第２、第３、第４、第５、第６又は第７の特徴における前記プログラムによる一連の手続を実録してなるリモートメンテナンス実施プログラムを記録した記録媒体の構成採用にある。

【００７３】本発明記録媒体の第２の特徴は、上記本発明プログラムの第７又は第９の特徴における前記プログラムによる一連の手続を実録してなるリモートメンテナンス実施プログラムを記録した記録媒体の構成採用にある。（請求項２５に対応）

【００７４】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態をそのシステム例、方法例、記録媒体例及びプログラム例について詳細を説明する。

【００７５】（システム例）図１に本発明の一実施形態であるリモートメンテナンス実施システム例の構成図を示す。リモートメンテナンスシステムは、インターネットゲートウェイ端末１（以下、情流ＧＷ端末）、内線端末２ａ～２ｎ（ｎは任意の自然数を表す）、保守サーバ３、リモートメンテナンス装置４、ＶＰＮゲートウェイ５（５ａ～５ｎ）の５つのノードからシステム構築される。

【００７６】前記情流ＧＷ端末１は、通常インターネット６（ＷＡＮ）側とローカルネットワークである内線（ＬＡＮ）７側のいずれともＴＣＰ／ＩＰで通信するこ

とを前提とする。また、保守サーバ３側のＬＡＮ８上のＶＰＮゲートウェイ５（５ａ～５ｎ）とＶＰＮを構築できる機能を持つことが必要がある。

【００７７】従来のルータｆやアプリケーションゲートウェイと呼ばれる物が対象となる。従来のＩＳＤＮターミナルアダプタのように、それ自体ではＴＣＰ／ＩＰの通信を行わない物は対象としない。以下の記述において、単に「端末」の呼称は、情流ＧＷ端末１を指す。

【００７８】前記内線端末２ａ～２ｎは、前記情流ＧＷ端末１配下の内線ＬＡＮ７に接続するＰＣ（パソコン）等の端末（群）である。内線ＬＡＮ７に接続されている情流ＧＷ端末１本体に含まれるサーバ部１０やルータ部１１も内線端末２ａ～２ｎとして扱う。前記保守センタ９は、保守サーバ３、リモートメンテナンス装置４、ＶＰＮゲートウェイ５（５ａ～５ｎ）を構成要素とするリモート保守を行うセンタの総称である。

【００７９】前記保守サーバ３は、情流ＧＷ端末１や内線端末２ａ～２ｎのリモートメンテナンスに関する情報を管理するインターネット６上のサーバで、インターネット６側とリモートメンテナンス装置４が存在するＬＡＮ８側に各々ＬＡＮインターフェースを持つ。

【００８０】前記リモートメンテナンス装置４は、情流ＧＷ端末１や内線端末２ａ～２ｎのリモートメンテナンスを行うオペレーティング装置で、ＷＥＢブラウザ機能を持つことが前提である。前記ＶＰＮゲートウェイ５ａ～５ｎは、インターネット６経由で、情流ＧＷ端末１と保守センタ９を結ぶＶＰＮを構築するためのＶＰＮゲートウェイ装置である。

【００８１】前記情流ＧＷ端末１は、ｈｔｔｐサーバ処理を行うｈｔｔｐサーバ部１００と、ｈｔｔｐサーバから呼ばれて内部処理を行うＣＧＩ処理部１０１と、ルータ部１１への制御コマンドを発行するルータ設定処理部１０２と、保守サーバ３にコマンドを送信するコマンド送出処理部１０３を含むサーバ部１０と、ＩＰｓｅｃを含んだＩＰルータ処理を制御するルータ部１１から構成される。

【００８２】前記保守サーバ３は、端末１からのｈｔｔｐコマンドを受信するｈｔｔｐサーバ部３０と、ｈｔｔｐサーバ部３０から呼ばれて内部処理を行うＣＧＩ処理部３１と、ＶＰＮゲートウェイ１へｔｅｌｎｅｔコマンドを発行するＶＰＮゲートウェイ設定処理部３２から構成される。前記ＶＰＮゲートウェイ５ａ～５ｎは、端末１のルータ部１１とＶＰＮセッションを行うＶＰＮ処理部５０と、保守サーバ３からのｔｅｌｎｅｔコマンドを受信する設定コマンド受信処理部５１から構成される。

【００８３】前記リモートメンテナンス装置４は、端末１のサーバ部１０へｈｔｔｐプロトコル等でコマンドを送出するメンテナンスコマンド処理部４０から構成される。以上、示した、保守サーバ３と、ＶＰＮゲートウェイ５ａ～５ｎと、リモートメンテナンス装置４を使って、保守センタ９からインターネット６のＶＰＮトンネル１２経由で、複数の情流ＧＷ端末１及びその内線端末２ａ～２ｎをリモートメンテナンスする際、情流ＧＷ端末１配下のローカルネットワークアドレスが如何なる場合でも、同時にＶＰＮリモートメンテナンスを実現する。

【００８４】（方法例）前記システム例に適用する本方法例におけるＶＰＮリモートメンテナンスは、設置通知処理と、ＶＰＮＧＷアドレス要求と、リモートメンテナンス要求処理と、リモートメンテナンス終了処理と、ＶＰＮＮＡＴ解放処理と、ＶＰＮ終了処理と、故障通知処理との７つの「通知コマンド及びレスポンス」と、実際に保守センタ９のオペレータが行う「リモートメンテナンス実施」（本リモートメンテナンスプロトコルにおいては、実際のメンテナンス作業のプロトコルについては、特に規定しない。それは、ＴＣＰ／ＩＰを利用していれば、汎用のアプリケーションであってもよいし、独自のプロトコルでもよい。）を通信プロトコルとして構成される。

【００８５】ここで、リモートメンテナンス実施以外の７つの通信プロトコルは実際のメンテナンス作業（以下、リモートメンテナンス実施）を行うための、手法にすぎず、あくまでも主旨は、以下の通りである。

【００８６】すなわち、第一の主旨は、リモートメンテナンス装置４からメンテナンス対象内線端末２ａ～２ｎに対して、ＶＰＮのトンネル１２を利用してＴＣＰ／ＩＰプロトコルを利用するアプリケーションで行い、このとき、保守センタ９のリモートメンテナンス装置４から、メンテナンス対象内線端末２ａ～２ｎへのＩＰ接続をＶＰＮＮＡＴ用ローカルＩＰアドレスを用いて、ルータ部１１内に機能構成する後記ＶＰＮＮＡＴ１１０で行うことにより、先に述べた複数の情流ＧＷ端末１へのアクセスをその配下のＩＰアドレスが重複している場合でも確実に実施することにある。ただし、当該ＮＡＴを経由すると実施不可能なアプリケーションは実施できないのは、制限事項である。

【００８７】また、第２の主旨は、リモートメンテナンス装置４からメンテナンス対象内線端末２ａ～２ｎに対して、ＶＰＮのトンネル１２を利用してＴＣＰ／ＩＰプロトコルを利用するアプリケーションで行い、このとき、保守センタ９のＶＰＮゲートウェイ５ａ～５ｎが増設などによりアドレスが変更された場合でも、リモートメンテナンス装置４から任意のＶＰＮゲートウェイ５ａ～５ｎ及びインターネットゲートウェイを介して、メンテナンス対象内線端末へのＩＰ接続が確実に実行されることにある。

【００８８】以下、前記第一の主旨を達成するための、本方法例を以下図面を参照して説明する。当該本方法例はルータ部１１内に機能構成するＶＰＮＮＡＴ１１０に動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与する

ことにある。図２をもとにＶＰＮＮＡＴ１１０に動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与する機能の概略を説明する。

【００８９】まず、①で保守センタ９にリモートメンテナンス対象端末の内線端末２ａ～２ｎ名を通知する。②で、保守センタ９は、情流ＧＷ端末１に対して、情流ＧＷ端末１のサーバ部１０経由でリモートメンテナンス対象内線端末２ａ～２ｎ名に対応するＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルＩＰアドレス（10.0.0.1）を付与する。これは、基本的にリモートメンテナンス要求の時点で行われる。

【００９０】次に③で、ＶＰＮＮＡＴ用ローカルＩＰアドレスとリモートメンテナンス対象内線端末２ａ～２ｎのＩＰアドレスを静的ＮＡＴ１１０で割り付ける。これも、②に引き続きリモートメンテナンス要求時に行われる。次に④でリモートメンテナンス実施時にＶＰＮトンネル１２の中を通してＶＰＮＮＡＴ用ローカルＩＰアドレスへアクセスする。そうすると、⑤に示すように、リモートメンテナンス対象内線端末２ａ～２ｎへパケットが転送されアクセス可能になる。

【００９１】このように事前に静的にＶＰＮＮＡＴ用ローカルＩＰアドレスを割り付けなくても動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与することにより、複数の情流ＧＷ端末１へのアクセスをその配下のＩＰアドレスが重複している場合でも同時に実施とすることができるようになる。

【００９２】以下、第２の主旨を達成する方法例として、ＶＰＮ構築に先立ち、保守センタ９がその配下の複数のＶＰＮゲートウェイ５ａ～５ｎからＶＰＮの空のリソースのあるＶＰＮゲートウェイ５ｉを動的に選択し、情流ＧＷ端末のルータ部１１に通知することにより、ルータ部１１内に設置されるＶＰＮゲートウェイのグローバルＩＰアドレスを動的にＶＰＮの対向ホストとして設定付与することにある。

【００９３】以下、本方法例を実現するための６つのプロトコルについて概要を説明する。前記設置通知処理は、情流ＧＷ端末１が設置されたことを保守サーバ３に通知し、保守サーバ３からリモートメンテナンスのための共有情報（ＩＰｓｅｃのPreshared Key、端末認証パスワード（以下、Secret（ID2））等）を暗号化して受け取ることが主旨である。

【００９４】また、前記主旨を実現するために、設置通知処理内でも、情流ＧＷ端末１のサーバ部１０とルータ部１１に対してＶＰＮＮＡＴ１１０を構築するのも本方法例においては大きな目的である。

【００９５】前記ＶＰＮＧＷアドレス要求処理は、保守サーバ３が保守センタ９配下の複数のＶＰＮゲートウェイ５ａ～５ｎからＶＰＮの空きのリソースのあるＶＰＮゲートウェイ５ｉを動的に選択して、そのＶＰＮゲートウェイ５ｉのグローバルＩＰアドレスをＶＰＮゲートウェイ通知レスポンスとして情流ＧＷ端末１に通知し、情流ＧＷ端末ルータ部１１は通知されたＶＰＮゲートウェイ５ｉのグローバルＩＰアドレスをＶＰＮの対向ホストとして設定を行うことも本方法においては大きな主旨である。

【００９６】前記リモートメンテナンス要求処理は、ＩＰｓｅｃによるリモートメンテナンスの実施を保守サーバ３に要求することを主旨とする。リモートメンテナンス要求処理に対応するメンテナンス対象端末は、情流ＧＷ端末１本体、及び、内線端末２ａ～２ｎとする。また、主旨を実現するために、リモートメンテナンス要求処理内でも、情流ＧＷ端末１のサーバ部１０とルータ部１１以外の内線端末２ａ～２ｎに対してＶＰＮＮＡＴ１１０を構築するのも本方法例においては大きな主旨である。

【００９７】前記リモートメンテナンス終了処理は、リモートメンテナンス装置４を使って実際にリモートメンテナンスが終了したことを対象となる情流ＧＷ端末１に伝えることを主旨とする。

【００９８】前記ＶＰＮＮＡＴ１１０解放処理は、リモートメンテナンスが終了した情流ＧＷ端末１のサーバ部１０とルータ部１１以外の内線端末２ａ～２ｎについてＶＰＮＮＡＴ１１０を解放することを目的とする。これにより、後の効果に述べるように、ＶＰＮＮＡＴ用ローカルＩＰアドレス資源を有効活用可能となる。ＶＰＮ終了処理は、ＩＰｓｅｃセッションを終了することを主旨とする。

【００９９】（プログラム例、記録媒体例）本方法例を実施するためのプログラム例及び記録媒体例を図面につき説明する。リモートメンテナンスの全体処理フロー図３～図９を用いて、各通信データの流れを示す。各図の“→”は、設置通知処理、ＶＰＮＧＷアドレス要求処理、リモートメンテナンス要求処理、リモートメンテナンス終了処理、ＶＰＮＮＡＴ解放処理、ＶＰＮ終了処理、故障通知処理の際の通信シーケンスにおけるコマンド送出及び受信を示した手順及び手続の流れである。

【０１００】処理形態は、情流ＧＷ端末１設置時に一度だけ、情流ＧＷ端末１設置者の操作を契機として、図３に示す設置通知処理の①設置通知コマンド（端末ＩＤ、公開鍵、原文、ＭＡＣ）→②設置通知レスポンス（暗号化Preshared Key、暗号化Secret ID2、暗号化保守者パスワード、暗号化サーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、暗号化ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、暗号化ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス）→③ルータ設定（ＶＰＮＮＡＴ１１０、暗号化Preshared Key）が行われる。

【０１０１】その後、内線端末２ａ～２ｎユーザ（以下、ユーザ）が情流ＧＷ端末１から保守センタ９（以下、センタ）に対して、内線端末２ａ～２ｎのリモートメンテナンスの要求をすると思い立った度毎に、内線端

末ユーザの操作を契機として、図４に示すＶＰＮＧＷアドレス要求の①ＶＰＮＧＷアドレス要求コマンド（端末ＩＤ、公開鍵、原文、ＭＡＣ）→②ＶＰＮＧＷ選択処理→③ＶＰＮＧＷアドレス要求レスポンス（ＶＰＮゲートウェイグローバルＩＰアドレス）→④ルータ設定（ＶＰＮゲートウェイグローバルＩＰアドレス）が行われる。

【０１０２】次に、ＶＰＮＧＷアドレス要求の処理終了を契機として、図５に示すリモートメンテナンス要求の①リモートメンテナンス要求コマンド（端末ＩＤ、内線端末２ａ～２ｎ名、情流ＧＷ端末グローバルアドレス、要求者レベル、緊急度、要求者名、電話番号、要求内容）→②ＶＰＮＮＡＴ用ローカルＩＰアドレス割り当て処理→③ＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティング設定→④ＩＰｓｅｃ設定処理→⑤リモートメンテナンス要求レスポンス（内線端末２ａ～２ｎ名、ＶＰＮＮＡＴ用ローカルＩＰアドレス、受付番号）→⑥ＶＰＮＮＡＴ用ローカルＩＰアドレスのＶＰＮＮＡＴ１１０設定が行われる。

【０１０３】センタ９では、オペレータがリモートメンテナンス装置４からリモートメンテナンス要求の受信を随時確認している。オペレータが、各々のリモートメンテナンス要求処理に対するリモートメンテナンスを実施すると思い立った度毎に、オペレータの操作により、図６に示す①リモートメンテナンス実施が行われる。

【０１０４】センタ９では、各々のリモートメンテナンス要求処理に対するリモートメンテナンスが終了した度毎に、オペレータの操作により、図７に示すリモートメンテナンス終了処理の①リモートメンテナンス終了コマンド（受付番号）→②リモートメンテナンス終了レスポンスが行われる。

【０１０５】リモートメンテナンス終了処理後、保守サーバ３の判断により、必要に応じて、自動的に、図８に示すＶＰＮＮＡＴ解放処理の①ＶＰＮＮＡＴ１１０解放コマンド（内線端末２ａ～２ｎ名）→②ＶＰＮＮＡＴ用ローカルＩＰアドレスＶＰＮＮＡＴ設定解除→③ＶＰＮＮＡＴ１１０解放レスポンス→④ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理→⑤ＶＰＮＮＡＴ用ローカルＩＰアドレスルーティング設定解除が行われる。

【０１０６】ＶＰＮＮＡＴ１１０解放終了後、保守サーバ３の判断により、必要に応じて、自動的に図９に示すＶＰＮ終了の①ＶＰＮ終了コマンド→②ＶＰＮＮＡＴ用ローカルＩＰアドレス初期化設定→③ＶＰＮ終了レスポンス→④ＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティング初期化→⑤ＩＰｓｅｃ設定解除が行われる。

【０１０７】以上が、全体フローの概略である。なお、情流ＧＷ端末１台に着目した場合の情流ＧＷ端末１及び保守センタ９の処理フローを図１０、図１１のフローチャートに示す。

【０１０８】即ち、図１０に示す情流ＧＷ端末１側フローチャートについては、設置通知ＳＴｃはＳＴａ→ＳＴｂを順次踏んで実践され、リモートメンテナンス終了処理ＳＴｈは設置通知ＳＴｃからＳＴｄ→ＳＴｅを踏んで、ＶＰＮＮＡＴ解放処理ＳＴｉは設置通知ＳＴｃからＳＴｄ→ＳＴｅ→ＳＴｆを踏んで、ＶＰＮ終了処理ＳＴｊは設置通知ＳＴｃからＳＴｄ→ＳＴｅ→ＳＴｆ→ＳＴｇを踏んで、故障通知ＳＴｎは設置通知ＳＴｃからＳＴｄ→ＳＴｋ→ＳＴＩを踏んで、ＶＰＮＧＷアドレス要求ＳＴｏは設置通知ＳＴｃからＳＴｄ→ＳＴｋを踏むか故障通知ＳＴｎから直結して踏んで、リモートメンテナンス要求ＳＴｍは設置通知ＳＴｃからＳＴｄ→ＳＴｋ→ＳＴｏを踏むかＳＴｄ→ＳＴｋ→ＳＴｌ→ＳＴｎ→ＳＴｏを踏んで、それぞれ実践され、その間必要に応じて繰り返しが入る。

【０１０９】図１１に示すセンタ９側フローチャート（情流ＧＷＩＤ＝Ｎ）については、設置通知処理ＳＴ６はＳＴ１→ＳＴ２→ＳＴ３を、ＶＰＮＧＷアドレス要求処理ＳＴ１６はＳＴ１→ＳＴ２→ＳＴ３→ＳＴ１５を、リモートメンテナンス要求処理ＳＴ７はＳＴ１→ＳＴ２→ＳＴ３→ＳＴ１５→ＳＴ４を、故障通知処理ＳＴ８はＳＴ１→ＳＴ２→ＳＴ３→ＳＴ１５→ＳＴ４→ＳＴ５を、それぞれ順次踏んで実践される。

【０１１０】リモートメンテナンス終了ＳＴ９はＳＴ１→ＳＴ２を踏んで、ＶＰＮＮＡＴ解放ＳＴ１２はリモートメンテナンス終了ＳＴ９からＳＴ１０→ＳＴ１１を踏んで、ＶＰＮ終了ＳＴ１４はＶＰＮＮＡＴ解放ＳＴ１２からＳＴ１３を踏んで、それぞれ実践され、その間必要に応じて繰り返しが入る。なお、図２６に示す故障通知は、故障発生時に通知されるが、全体の流れとは独立な処理なのでここでは詳細にはふれない。

【０１１１】［リモートメンテナンス実施のための前提条件］なお、本実施形態例を実行するためには、以下の前提条件が必要である。

（１）保守サーバ３と端末１では、共有秘密情報（以下、Secret（ID））を事前に共有していること。Secret（ID）は、出荷時に端末１にＲＯＭ等に埋め込み、保守サーバ３と共有することで対応する。なおSecret（ID）は、保守サーバ３がリモートメンテを行うすべての端末１に共通とする。

【０１１２】（２）端末１のルータ部１１は、ＩＰｓｅｃ等のＩＰレベルのＶＰＮ機能を持つこと。また、ＶＰＮセッションについて、セッション待ち受け側の設定を事前に行っておくこと（ＩＰｓｅｃの場合は、レスポンダとして設定しておくこと）。また、Preshared keyはダミーデータを設定しておくこと。

（３）保守センタ９のＶＰＮゲートウェイ５は、ＶＰＮセッションについて、セッション確立側の設定を事前に行っておくこと（ＩＰｓｅｃの場合は、イニシエータとして設定しておくこと）。

【０１１３】（４）ＶＰＮゲートウェイ５は、端末１のルータ部１１と通信互換性のあるＶＰＮ機能を持つこ

と。
（５）端末１のルータ部１１は、保守サーバ３の公開されたグローバルＩＰアドレス（または、インターネットホスト名）を設置通知の時点までに事前に知っていること。また、インターネット６へ接続設定が完了していること。
【０１１４】（６）ルータ設定処理部１０２からルータ部１１への各種設定はリモートコンソール（以下、ｔｅｌｎｅｔ）、またはプロセス間通信（ソケット通信等）で行えること。
（７）保守サーバ３のＶＰＮゲートウェイ設定処理部３２からＶＰＮゲートウェイ５の設定コマンド受信処理部５１への各種設定はｔｅｌｎｅｔまたはプロセス間通信（ソケット通信等）で行えること。
【０１１５】（８）保守サーバ３上には、ＶＰＮＮＡＴ１１０ＤＢを持つ。テーブルは、ＶＰＮＮＡＴ用ローカルＩＰアドレスをキーとした複数レコードから構成され、フィールドとして、割り当て情流ＧＷ端末ＩＤ／端末名を持つ。
（９）情流ＧＷ端末１には、ホストテーブルを持つ。テーブルは、内線端末２ａ～２ｎ名をキーとした複数レコードから構成され、フィールドとして、実ＩＰアドレス、ＶＰＮＮＡＴ用ローカルＩＰアドレスを持つ。初期状態では、ホストテーブルは空である。
【０１１６】（１０）保守サーバ３上のＶＰＮＧＷ５（５ａ～５ｎ）は複数の存在を可能とする。一つのＶＰＮＧＷ５はそのＶＰＮＧＷ５が許容する複数個のＶＰＮトンネル１２を構成可能とする。
（１１）保守サーバ３上にはＶＰＮＧＷトンネルテーブルを持つ。テーブルは、ＶＰＮゲートウェイ５のＩＰアドレス及びＶＰＮトンネル番号をキーとした複数のレコードから構成され、フィールドの値として、割り当て情流ＧＷＩＤを持つ。
【０１１７】［処理シーケンスの説明］以下、図３～図９と、図１２～図２５を用いて、各処理の手順について詳細を説明する。書中左に振っている番号ｎ－ｎ（ｎは任意の自然数）は、図中のステップ処理番号に対応する。
【０１１８】＜設置通知処理＞図３、図１２及び図１３に示すよう設置通知は、端末１が設置されたことを保守サーバ３に通知し、保守サーバ３からリモートメンテナンスのための共有情報（ＩＰｓｅｃのPreshared Key、端末１認証パスワード（以下、Secret（ID2））、保守者パスワード）を暗号化して受け取り、それを設定することが目的である。
【０１１９】設置通知処理以降の端末認証処理にSecret（ID）の代わりに、Secret（ID2）を使うのは、端末１全てに共通であるSecret（ID）よりも、Secret（ID2）を使った方がセキュリティが強化されるためである。また、ＶＰＮを構築する際、各情流ＧＷ端末１配下のプライベートＩＰアドレスの重複が考えられるため、それを避けるために、ＶＰＮＮＡＴ処理を行う。そのための、ＶＰＮ用ダミープライベートＩＰアドレス（以下、ＶＰＮＮＡＴ用ローカルＩＰアドレス）を保守サーバ３から受け取ることが第２の目的である。
【０１２０】①設置通知コマンド（端末サーバ部１０→保守センタ９）
((通信契機))
１－１　端末１設置終了後、ルータ部１１がインターネット６への接続設定が完了した時点で、サーバ部１０に対するボタン操作により行う。設置通知は一度だけ行えばよい。
【０１２１】((端末前処理))
１－２　サーバ部１０のコマンド送出処理部１０３は、秘密鍵と公開鍵を生成する。アルゴリズムにはＲＳＡ等の公開鍵暗号を使用する。
１－３　「端末１のユニークなＩＤ＋タイムスタンプ」から認証のための原文を作成する。
１－４　原文に対して、Secret（ID）を用いたメッセージ認証子（ＭＡＣ）を生成する（ISO9797－1、ISO9797－2に準拠することが望ましい）。
【０１２２】((コマンド送信処理))
１－５　端末ＩＤ、公開鍵、原文、ＭＡＣをパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非ＩＰｓｅｃセッション＞として設置通知コマンドを送信する。
【０１２３】②設置通知レスポンス（保守サーバ３→端末サーバ部１０）
((保守サーバ処理))
１－６　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡し、ＣＧＩ処理部３１は、原文に対して、Secret（ID）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末１と同様の演算）、受信したＭＡＣと一致することを確認する（端末認証）。
【０１２４】１－７　ＣＧＩ処理部３１は、ＩＰｓｅｃの認証鍵（Preshared Key）、Secret（ID2）をランダムに生成し、保守者パスワードを設定ファイルから取得し、端末ＩＤＢの中の端末ＩＤに対応するレコードを新規にクリエイトし（既に存在する場合は上書き）、該当レコードの各フィールドに保持する。
【０１２５】１－８　ＣＧＩ処理部３１は、ＶＰＮＮＡＴＤＢ９１から空きＶＰＮＮＡＴ用ローカルＩＰアドレスをサーバ部１０用とルータ部１１用に二つ選択し、該当レコードの割り当て状況フィールドに情流ＧＷ端末ＩＤ／端末名を保持するとともに、端末１ＤＢのサーバ部１０ＶＰＮＮＡＴ用ローカルＩＰアドレス及びルータ部１１ＶＰＮＮＡＴ用ローカルＩＰアドレスフィールドにＶＰＮＮＡＴ用ローカルＩＰアドレスを保持する。

【０１２６】１－９　ＣＧＩ処理部３１は、ＩＰｓｅｃの認証鍵（Preshared Key）、Secret（ID2）、保守者パスワード、サーバ部１０及びルータ部１１用ＶＰＮＮＡＴ用ローカルＩＰアドレスを、情流ＧＷ端末１の公開鍵で暗号化する。

【０１２７】（(レスポンス送信処理)）

１－１０　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常またはエラーステータス（認証異常等））、端末１の公開鍵で暗号化したＩＰｓｅｃの認証鍵（Preshared Key）、端末１の公開鍵で暗号化したSecret（ID2）、端末１の公開鍵で暗号化した保守者パスワード、端末１の公開鍵で暗号化したサーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、端末１の公開鍵で暗号化したルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレスをパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３０）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

【０１２８】③サーバ部１０とルータ部１１のＶＰＮＮＡＴ１１０設定（端末サーバ部１０→端末ルータ部１１）

((端末後処理))

１－１１　端末サーバ部１０は、端末１の秘密鍵で、ＩＰｓｅｃの認証鍵（Preshared Key）、Secret（ID2）、保守者用パスワード、サーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレスを復号化し、保持する。

【０１２９】１－１２　端末サーバ部１０は、ＶＰＮゲートウェイ５をＩＰｓｅｃ対象ホストとしたPreshared Key、サーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレスの設定コマンド（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる）を作成する。この時、ＶＰＮゲートウェイのアドレスはダミーで設定する。

【０１３０】((コマンド送信処理))

１－１３　前の処理で作成したコマンドをパラメータとして、端末（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

((端末ルータ部処理))

１－１４　受信したPreshared Keyの設定及びＶＰＮＮＡＴ１１０の設定をルータ部１１に書き込む。

【０１３１】((レスポンス送信処理))

１－１５　ステータス（正常またはエラーステータス（コマンド異常等））をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

((端末ルータ設定部後処理))なし上記で設置通知処理が完了となる。

【０１３２】＜故障通知処理＞図２６のシーケンス図と図２７の処理フローの手順図を示すよう、故障通知処理は、端末１が故障したことを検知し、保守サーバ３に通知する。端末１（サーバ部１０）では、端末１のサーバ部１０及びルータ部１１の故障の発生、復旧を常時監視して、故障が発生したら故障通知処理を起動する。即ち、故障通知処理の①故障通知コマンド（端末ＩＤ、原文、ＭＡＣ、故障コード）→②故障通知レスポンス→③リモートメンテナンス要求起動が行われる。

【０１３３】((通信契機))

７－１　端末１で故障発生を検知した場合、端末１が自律的に行う。

((端末前処理))

７－２　「端末１のユニークなＩＤ＋タイムスタンプ」から認証のための原文を作成する。

７－３　原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成する（ISO9797－1、ISO9797－2に準拠することが望ましい）。

【０１３４】((コマンド送信処理))

７－４　端末ＩＤ、原文、ＭＡＣ、故障のコードをパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非ＩＰｓｅｃセッション＞として故障通知コマンドを送信する。

【０１３５】((保守サーバ処理))

７－５　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡す。ＣＧＩ処理部３１は、原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末１と同様の演算）、受信したＭＡＣと一致することを確認する（端末認証）。

７－６　ＣＧＩ処理部３１は、受信した故障コードを保持する。

【０１３６】((レスポンス送信処理))

７－７　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常またはエラーステータス（認証異常等））をパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

【０１３７】((端末後処理))

７－８　ＶＰＮＧＷアドレス要求処理を起動する。

なお、故障通知処理によって保持した故障コードは、リモートメンテナンス装置４からｈｔｔｐアクセス等で参照できることが望ましい（故障確認処理）。

【０１３８】＜ＶＰＮＧＷアドレス要求処理＞図４のシーケンス図及び図１４、図１５の処理フロー手順のように、ＶＰＮＧＷアドレス要求は、保守サーバ３が選択し

た保守センタ９のＶＰＮゲートウェイ５ｉのアドレスを情流ＧＷ端末１に通知することを主旨とする。基本的には、内線端末２ａ～２ｎから情流ＧＷ端末１にリモートメンテナンス要求の登録があった時点で、ＶＰＮＧＷアドレス要求が通知されるものの、端末管理者が情流ＧＷ端末１本体のボタン操作でＶＰＮＧＷアドレス要求を通知することも可能とする。

【０１３９】①ＶＰＮＧＷアドレス要求コマンド（端末サーバ部１０→保守サーバ３）

（通信契機）

９－１　内線端末２ａ～２ｎから情流ＧＷ端末１へのＷＥＢアクセス又は端末管理者のボタン操作などによる情流ＧＷ端末１へのアクションによる。

【０１４０】（端末前処理）

９－２　内線端末２ａ～２ｎからのブラウザアクセスにより起動される場合は、リモートメンテナンス要求で必要な情報である「要求者名、要求者レベル、内線端末名（複数設定可）、緊急度、電話番号、要求内容」をブラウザから入力させることにより、取得し、リモートメンテナンス情報として保持する。画面イメージでは、ブラウザ画面の通りである。情流ＧＷ端末１のボタン操作により起動される場合は、「要求者名、要求者レベル、端末名、緊急度、電話番号、要求内容」を事前に登録されたテーブルから取得し、保持する。要求者レベルは、一般又は管理者を設定可能とする。尚、内線端末名は、リモートメンテナンス対象としたい内線端末の名称であり、他の情報は、保守センタ９のオペレータが、リモートメンテナンス要求を起動したユーザがセンタ９のオペレータにリモートメンテナンスを実施してもらうにあたり、その意向を示すための情報である。

【０１４１】９－３　サーバ部１０のコマンド送出処理部１０３は、秘密鍵と公開鍵を生成する。アルゴリズムにはＲＳＡ等の公開鍵暗号を使用する。

９－４　「端末のユニークなＩＤ＋タイムスタンプ」から認証のための原文を生成する。

９－５　原文に対して、Ｓｅｃｒｅｔ（ｉｄ２）を用いたメッセージ認証子（ＭＡＣ）を生成する。（ＩＳＯ９７９７－１，ＩＳＯ９７９７－２）に準拠することが望ましい。）

【０１４２】（コマンド送信処理）

９－６　端末ＩＤ，原文，ＭＡＣ，公開鍵をパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非Ｉｐｓｅｃセッション＞としてリモートメンテナンス要求コマンドを送信する。

【０１４３】②ＶＰＮＧＷ選択処理

（保守サーバ処理部）

９－７　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡す。ＣＧＩ処理部３１は、原文に対して、Ｓｅｃｒｅｔ（ｉｄ２）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末１と同様の演算）、受信したＭＡＣと一致することを確認する。（端末認証）

【０１４４】９－８　保守サーバ３はＶＰＮＧＷトンネルＤＢを読み出し、ＶＰＮＧＷトンネルＤＢの割り当て状況のトンネルを先頭から検索し、フィールドの値が「未使用」のトンネル番号を取得する。また、当該取得したトンネル番号に対応するフィールドを「未使用」から「端末ＩＤ」に書き換え、対応するＶＰＮＧＷグローバルＩＰアドレスを取得する。以下、このグローバルＩＰアドレスに対応するＶＰＮＧＷを「５ｉ」とする。ここで示したＶＰＮゲートウェイ５ａ～５ｎの選択処理は、本発明の特徴の一つである。

【０１４５】９－９　レスポンスのパラメータの前記「ＶＰＮＧＷグローバルＩＰアドレス」を受信した公開鍵で暗号化する。

【０１４６】③ＶＰＮＧＷアドレス要求レスポンス（保守サーバ３→端末サーバ部１０）

（レスポンス送信処理）

９－１０　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常又はエラーステータス（認証異常等））、端末１の公開鍵で暗号化したＶＰＮＧＷグローバルＩＰアドレスをパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３０）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非セッション＞としてレスポンスを送信する。

【０１４７】④ＶＰＮＮＧアドレス要求レスポンス受信後処理（端末サーバ部１０→端末ルータ部１１）

（端末前処理）

９－１１　端末サーバ部１０は、端末１の秘密鍵で、ＶＰＮＧＷグローバルＩＰアドレスを復号化し、保持する。

【０１４８】９－１２　端末サーバ部１０は、ＶＰＮＧＷグローバルＩＰアドレスをＶＰＮ対向ホストとして設定するためのコマンド（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる。）を作成する。

９－１３　前の処理で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

【０１４９】（端末ルータ部処理）

９－１４　ＶＰＮＧＷグローバルアドレスをＶＰＮ対向ホストとする設定をルータ部１１に書き込む。

（レスポンス送信処理）

９－１５　ステータス（正常又はエラーステータス（コマンド異常等））をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜非Ｉｐｓｅｃ

セッション>としてレスポンスを送信する。
【０１５０】（端末ルータ設定部後処理）
９－１６　リモートメンテナンス要求処理を起動する。以上によりＶＰＮＧＷアドレス要求処理が完了となる。この本処理が発明のポイントの一つである。
【０１５１】<リモートメンテナンス要求処理>図５のシーケンス図と図１６乃至図１９の処理フローの手順図に示すよう、リモートメンテナンス要求処理は、ＩＰｓｅｃによるリモートメンテナンスの実施を保守サーバ３に要求することを主旨とする。
【０１５２】また、リモートメンテナンス要求処理では、ＶＰＮを構築するための情流ＧＷ端末１のＩＰアドレスをセンタ９に通知することも主旨の一つである。リモートメンテナンス要求は、ｈｔｔｐプロトコルで行われその環境変数から、保守サーバ３は、情流ＧＷ端末１に受信したＩＰアドレスを取得する。そのＩＰアドレスをもとに保守センタ９のＶＰＮゲートウェイ５ｉに対して、ＶＰＮ鍵、端末ＩＰアドレスを設定する。
【０１５３】更に、ＶＰＮを構築する際、各情流ＧＷ端末１配下の内線端末２ａ～２ｎに対してＩＰレベルの通信を行えるようにするために、センタ９からリモートメンテナンス対象内線端末２ａ～２ｎに対するＶＰＮＮＡＴ用ローカルＩＰアドレスを取得し、ＶＰＮＮＡＴ処理を行う。
【０１５４】ＶＰＮＮＡＴ処理を行うことにより、情流ＧＷ端末１配下のローカルＬＡＮアドレスが同一である複数の情流ＧＷ端末１へのメンテナンスを行う場合でも（例えば、メンテナンス対象の情流ＧＷ端末１が二つ存在し、二つの情流ＧＷ端末１が共に192.168.0.0/24のローカルネットを持つような場合）、保守センタ９のオペレータ端末から情流ＧＷ端末１及びその配下の内線端末２ａ～２ｎに対してＩＰリチャーブルな環境を構築できる。
【０１５５】①リモートメンテナンス要求コマンド（端末サーバ部１０→保守サーバ３）
((通信契機))
２－１　ＶＰＮＧＷアドレス要求の処理終了後に、起動される。
【０１５６】((端末前処理))
２－２　ＶＰＮＧＷアドレス要求で保持したリモートメンテナンス情報を取得する。
【０１５７】２－３　サーバ部１０のコマンド送出処理部１０３は、秘密鍵と公開鍵を生成する。アルゴリズムにはＲＳＡ等の公開鍵暗号を使用する。
２－４　「端末１のユニークなＩＤ＋タイムスタンプ」から認証のための原文を作成する。
【０１５８】２－５　原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成する（ISO9797－1、ISO9797－2に準拠することが望ましい）。
２－６　保守センタ９に通知するためのパラメータのうち、「要求者名、内線端末名、電話番号、要求内容」を情流ＧＷ端末１に保持されているSecret（ID2）で暗号化する。
【０１５９】((コマンド送信処理))
２－７　端末ＩＤ、原文、ＭＡＣ、公開鍵、要求者レベル、緊急度、暗号化要求者名、暗号化内線端末名（複数可）、暗号化電話番号、暗号化要求内容をパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで<非ＩＰｓｅｃセッション>としてリモートメンテナンス要求コマンドを送信する。
【０１６０】②ＶＰＮＮＡＴ用ローカルＩＰアドレス割り当て処理
((保守サーバ処理))
２－８　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡す。ＣＧＩ処理部３１は、原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末と同様の演算）、受信したＭＡＣと一致することを確認する（端末認証）。
【０１６１】２－９　ＣＧＩ処理部３１は、受付番号を生成し、リモートメンテナンス要求ＤＢ９２のレコードを新規にクリエイトし、受付番号、受信時刻、メンテナンス状態（この時点では、常に対応待ち）を保守端末ブラウザの端末ＤＢ９０に保持する。また、テーブル名には、要求者レベルが管理者の場合は、「管理者」として保持し、要求者レベルが一般の場合は、内線端末２ａ～２ｎ名を保持する。なお、端末ＤＢ９０のレコードを図２６に示す。
【０１６２】２－１０　ＣＧＩ処理部３１は、環境変数REMOTE_ADDRから情流ＧＷ端末１のグローバルＩＰアドレスを取得し、前記リモートメンテナンス要求ＤＢ９２のレコードに保持する。
２－１１　ＣＧＩ処理部３１は、端末ＩＤ、要求者レベル、緊急度を前記リモートメンテナンス要求ＤＢ９２のレコードに保持する。
【０１６３】２－１２　ＣＧＩ処理部３１は、暗号化内線端末名、暗号化要求者名、暗号化電話番号、暗号化要求内容をSecret（ID2）で復号化し前記リモートメンテナンス要求ＤＢ９２のレコードに保持する。なお、リモートメンテナンス要求ＤＢ９２のレコードを図２７に示す。
【０１６４】２－１３　ＣＧＩ処理部３１は、通知された端末ＩＤ／内線端末名（複数端末名が存在する場合は、それぞれの端末名について）をキーとして、ＶＰＮＮＡＴＤＢ９１を検索し、その端末ＩにＶＰＮＮＡＴ用ローカルＩＰアドレスが割り当てられているかどうかを判断する。
【０１６５】ＶＰＮＮＡＴ用ローカルＩＰアドレスが割り当てられていれば、割り当て済みのＶＰＮＮＡＴ用ロ

ーカルＩＰアドレスを前記リモートメンテナンス要求ＤＢ９２のレコードに保持し、ＶＰＮＮＡＴ用ローカルＩＰアドレスが割り当てられていなければ、ＶＰＮＮＡＴＤＢ９１から空きＶＰＮＮＡＴ用ローカルＩＰアドレスを選択する。

【０１６６】該当レコードの割り当て状況フィールドに情流ＧＷ端末ＩＤ／内線端末名を保持するとともに、保持したＶＰＮＮＡＴ用ローカルＩＰアドレスを前記リモートメンテナンス要求ＤＢ９２のレコードにも保持する。なお、ＶＰＮＮＡＴＤＢ９１のレコードを図３０に示す。

【０１６７】２－１４　ＣＧＩ処理部３１は、リモートメンテナンス装置４のＷＥＢブラウザ上に、リモートメンテナンス要求を受信した旨を表示できるようにページを作成する。表示内容は、受付番号、端末ＩＤ、グローバルＩＰアドレス、要求者名、要求者レベル、電話番号、緊急度、要求内容、受信時刻、ＶＰＮＮＡＴ用ローカルＩＰアドレス、テーブル名、メンテナンス状態を表示する（図２９参照）。

【０１６８】⑤リモートメンテナンス要求レスポンス処理（保守サーバ３→端末サーバ部１０）

（保守サーバ部）

２－２６　レスポンス処理の内、「内線端末名とダミーＩＰアドレスの組」を受信した公開鍵で暗号化する。

（レスポンス送信処理）

２－２７　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常又はエラーステータス（認証異常等））、受付番号、端末１の公開鍵で暗号化した内線端末名とＶＰＮＮＡＴ用ローカルＩＰアドレスの組（複数可）をパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３０）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非Ｉｐｓｅｃセッション＞としてレスポンスを送信する。

【０１６９】③ＩＰｓｅｃ処理対象パケット設定（保守センタ９→ＶＰＮゲートウェイ５ｉ）

（コマンド送信処理）

２－１５　ＶＰＮゲートウェイ設定処理部３２は、リモートメンテナンス要求ＤＢの該当レコードから、端末ＩＤおよび②の処理で保持したＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを取得する。

２－１６　ＶＰＮゲートウェイ設定処理部３２は、ＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを端末ＩＤに対応したＶＰＮトンネル１２に割り付けるための設定（ＶＰＮゲートウェイ５ｉのｔｅｌｎｅｔコマンドの実装により異なる。）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。

【０１７０】（ＶＰＮゲートウェイ処理）

２－１７　受信したＶＰＮＮＡＴ用ローカルＩＰアドレスをＩＰｓｅｃ処理対象ホストとするための設定をＶＰＮゲートウェイ５ｉに書き込む。

（レスポンス送信処理）

２－１８　ステータス（正常又はエラーステータス（コマンド異常など））をパラメータとして、ＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。

【０１７１】（ＶＰＮゲートウェイ設定処理部後処理）

２－１９　ＶＰＮゲートウェイ設定処理部３２は、「①リモートメンテナンス要求コマンド」で受信した端末ＩＤを持つ情流ＧＷ端末１との間にＶＰＮが確立しているかをＶＰＮゲートウェイ５ｉから取得する。

２－２０　ＶＰＮゲートウェイ５ｉのＶＰＮ確立状況より、ＶＰＮが確立している場合は、プロセスを終了する。ＶＰＮが確立していない場合は、④ＩＰｓｅｃ設定処理を起動する。

【０１７２】④ＩＰｓｅｃ設定処理（保守センタ９→ＶＰＮゲートウェイ５ｉ）

（ＶＰＮゲートウェイ設定処理部前処理）

２－２１　保守サーバ３／ＣＧＩ処理部３１からＩＰｓｅｃの認証鍵（ＰｒｅｓｈａｒｅｄＫｅｙ）、端末ルータ部１１のグローバルＩＰアドレスを取得し、コマンドを生成する。

【０１７３】（コマンド送信処理）

２－２２　端末ルータ部１１のグローバルＩＰアドレスをＩＰｓｅｃ対象ホストとしたＰｒｅｓｈａｒｅｄｋｅｙの設定及び端末ＩＤに対応したＶＰＮトンネル１２を確立するための設定（ＶＰＮゲートウェイ５ｉのｔｅｌｎｅｔコマンドの実装により異なる。）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。

【０１７４】（ＶＰＮゲートウェイ処理）

２－２３　受信したＰｒｅｓｈａｒｅｄｋｅｙ及びＶＰＮトンネル１２を確立するための設定をＶＰＮゲートウェイ５ｉに書き込む。

（レスポンス送信処理）

２－２４　ステータス（正常又はエラーステータス（コマンド異常など））をパラメータとして、ＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。

【０１７５】（保守サーバ後処理）

２－２５　ＶＰＮゲートウェイ設定処理部３２は、「①

リモートメンテナンス要求コマンド」で受信した端末ＩＤを持つ情流ＧＷ端末１との間にＶＰＮの確立が完了しているかをＶＰＮゲートウェイ５ｉから取得する。確立が完了していない場合は、数秒間隔でＶＰＮ確立の完了を確認するまで同様の取得処理を繰り返す。ＶＰＮの確立完了が確認できた時点で、⑤リモートメンテナンス要求レスポンス処理を起動する。尚、ＶＰＮ設定が完了した段階で、その状態が、リモートメンテナンス装置４から確認できることが望ましい。理由は、ＶＰＮ設定が完了したことを確認した上で、⑥リモートメンテナンス開始指示を行えた方が保守者の作業効率がよいからである。

【０１７６】⑥サーバ部１０とルータ部１１のＶＰＮＮＡＴ設定（端末サーバ部１０→端末ルータ部１１）

（端末処理部）

２－２８　リモートメンテナンス要求レスポンスを受信した端末サーバ部１０は、受付番号を保持する。

２－２９　端末サーバ部１０は、端末１の秘密鍵で、内線端末名とＶＰＮＮＡＴ用ローカルＩＰアドレスの組（複数の場合あり）を復号化し、ホストテーブルに保持する。

【０１７７】２－３０　端末サーバ部１０は、内線端末名をキーとして、端末サーバ部１０がもつている内線端末名と実ＩＰアドレスの組のテーブル（ＤＮＳなどで参照）から端末名に対応する実ＩＰアドレスを取得し、端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスと実ＩＰアドレスをＶＰＮＮＡＴ１１０で対応付ける設定コマンド（複数の場合あり）（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる。）を作成する。

（コマンド送信処理）

２－３１　２－３０で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

【０１７８】（端末ルータ部処理）

２－３２　ＶＰＮＮＡＴ１１０の設定をルータ部１１に書き込む。

（レスポンス送信処理）

２－３３　ステータス（正常又はエラーステータス（コマンド異常等））をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０２）へのｔｅｌｎｅｔレスポンス＜非Ｉｐｓｅｃセッション＞としてレスポンスを送信する。

（端末ルータ設定部後処理）なし

以上により、リモートメンテナンス要求処理が完了となる。

【０１７９】＜リモートメンテナンス実施処理＞

（リモートメンテナンス装置４→内線端末２ａ～２ｎ）

図６のシーケンス図及び図１９の手順フロー図に示すように、リモートメンテナンス実施処理は、前記リモートメンテナンス要求処理を受けて、ＩＰｓｅｃ等のＶＰＮによるトンネル１２を経由してリモートメンテナンス装置４から情流ＧＷ端末１本体及びその内線端末２ａ～２ｎに対してセキュアなリモートメンテナンスを行い（ＶＰＮ経由で行うため、伝送路が暗号化できる）、端末１の故障の復旧、パソコンへのアプリケーションのリモートインストール等を実施することを主旨とする。

【０１８０】リモートメンテナンス装置４は、特殊なものではなく、ローカルネットワーク８上で内線端末２ａ～２ｎに対してコマンドを送出することにより、内線端末２ａ～２ｎをメンテナンスできる装置であればそれを転用できる。機能としては、故障（例えば、Proxy故障）について、復旧動作（proxyの起動、端末１の再起動）を行い故障を復旧する。また、端末１のログの表示や、ルータ部１１の設定の確認も行える。ツールとしては、ｈｔｔｐクライアント（ＷｅＢブラウザ）や、ｔｅｌｎｅｔツール等である。

【０１８１】また、パソコンに対するリモートインストールについては、ＶＮＣ等の遠隔制御ソフト等による。従って、この処理は、リモートメンテナンス装置４から、メンテナンスを行う内線端末２ａ～２ｎへの通信プロトコルに依存した汎用的なものであるため、詳しくは言及しない。

【０１８２】繰り返しになるが、センタ９から内線端末２ａ～２ｎへの接続は、リモートメンテナンス要求時に付与したＶＰＮＮＡＴ用ローカルＩＰアドレスに対して行うことが本実施形態例のポイントである。

【０１８３】①リモートメンテナンス開始処理(リモートメンテナンス装置４→保守サーバ３)

((通信契機))ＶＰＮトンネル１２が張られている状態において、リモートメンテナンス装置４（図中保守端末）上のＷＥＢブラウザから、リモートメンテナンス保守者の任意の契機で起動される（前述した故障確認処理で故障を検知した時点でも、それに同期して起動するのが望ましい）。

【０１８４】((リモートメンテナンス開始処理))

３－１　保守サーバ３のリモートメンテナンス要求確認画面にアクセスし、対象とするリモートメンテナンス要求に対するリモートメンテナンスを開始したことをＣＧＩ処理部３１で、保守サーバ３に通知する。

【０１８５】((サーバ処理))

３－２　ＣＧＩ処理部３１でリモートメンテナンス開始を起動されると、リモートメンテナンス要求ＤＢ９２の該当テーブルのメンテナンス状態が「対応中」となる。

【０１８６】②リモートメンテナンス実施処理（リモートメンテナンス装置４→内線端末２ａ～２ｎ）

((リモートメンテンナンス実施))

３－３　リモートメンテナンスを実施する。リモートメンテナンスでは、リモートメンテナンス要求を受けたＶ

ＰＮＮＡＴ用ローカルＩＰアドレスに対してＶＰＮ経由でＩＰ接続を行う。リモートメンテナンス実施時には、リモートメンテナンス要求ＤＢ９２を参照しながら作業を行えるようにサーバ側のユーザインタフェースを設計することを強く推奨する。

【０１８７】＜リモートメンテナンス終了処理＞図７のシーケンス図と図２０の手順フロー図に示すよう、リモートメンテナンス終了処理は、リモートメンテナンス要求で要求されたリモートメンテナンス作業が終了したことを、保守サーバ３から情流ＧＷ端末１に伝えることを主旨とする。

【０１８８】①リモートメンテナンス終了コマンド送信処理（保守サーバ３→端末サーバ部１０）

((通信契機))

４－１　ＶＰＮトンネル１２が張られている状態において、要求されたリモートメンテナンス作業が終了した時点で、リモートメンテナンス装置４上のＷＥＢブラウザから保守サーバ３に対するリモートメンテナンス保守者によるＣＧＩ処理部３１のキックで起動される。

【０１８９】((サーバ前処理))

４－２　ＣＧＩ処理部３１でリモートメンテナンス終了を起動されると、リモートメンテナンス要求ＤＢ９２の該当テーブルのメンテナンス状態が「終了」となる。なお、図３１にリモートメンテナンス要求ＤＢ９２のテーブルレコードを示す。

【０１９０】４－３　保守サーバ３は、リモートメンテナンス要求ＤＢ９２の該当テーブルのメンテナンス状態が「終了」となったこと検知すると、受付番号ををパラメータとして、該当テーブルの受付番号を取得し、受付番号をパラメータとしてリモートメンテナンス終了コマンドを作成する。この受付番号は、後に説明するＶＰＮＮＡＴ１１０解放処理及びＶＰＮ終了処理でも参照される。

【０１９１】((コマンド送信処理))

４－４　前の処理で作成したコマンドをパラメータとして保守サーバ３から端末１（ｈｔｔｐサーバ部１００）へのｈｔｔｐコマンドで＜ＩＰｓｅｃセッション＞としてリモートメンテナンス終了コマンドを送信する。

【０１９２】②リモートメンテナンス終了コマンド受信処理（端末サーバ部１０→保守サーバ３）

((端末サーバ部処理))

４－５　リモートメンテナンス終了を受信すると、パラメータから受付番号を抽出し、保持していた受付番号の状態を終了とする。

【０１９３】((レスポンス送信処理))

４－６　端末１のｈｔｔｐサーバ部１００は、ステータス（正常またはエラーステータス）をパラメータとし、端末１（ｈｔｔｐサーバ部１００）から保守センタ９へのｈｔｔｐレスポンス＜ＩＰｓｅｃセッション＞としてレスポンスを送信する。

【０１９４】③リモートメンテナンス終了レスポンス受信後処理（保守サーバ３）

((サーバ後処理))

４－７　レスポンス受信後、該当内線端末２ａ～２ｎに対するメンテナンスが全て終了したかを判断し、該当内線端末２ａ～２ｎに対するメンテナンスが全て終了していなかったら処理を終了する。該当内線端末２ａ～２ｎに対するメンテナンスが全て終了ていたら、さらに、終了した内線端末は情流ＧＷ端末１のサーバ部１０又はルータ部１１かを判断し、端末１のサーバ部１０又はルータ部１１でない場合は、ＶＰＮＮＡＴ解放処理を起動する。

【０１９５】端末１のサーバ部１０又はルータ部１１の場合は、対応する情流ＧＷ端末１に対するリモートメンテナンスを全て終了したかを判断し、全て終了していたら、ＶＰＮ終了処理を起動し、全て終了していなかったら、処理を終了する。以上で、リモートメンテナンス終了処理が完了となる。

【０１９６】＜ＶＰＮＮＡＴ解放処理＞図８のシーケンス図及び図２１、図２２の手順フロー図に示すよう、ＶＰＮＮＡＴ１１０解放処理は、リモートメンテナンス要求時に保守センタ９から情流ＧＷ端末１に割り振られたＶＰＮＮＡＴ用のＶＰＮＮＡＴ用ローカルＩＰアドレスを解放することを主旨とする。

【０１９７】①ＶＰＮＮＡＴ１１０解放コマンド送信処理（保守サーバ３→端末サーバ部１０）

((通信契機))

５－１　ＶＰＮトンネル１２が張られている状態において、リモートメンテナンス終了後、該当内線端末２ａ～２ｎに対するメンテナンスが全て終了し、その内線端末２ａ～２ｎが情流ＧＷ端末１のサーバ部１０又はルータ部１１以外の場合に起動される。

【０１９８】((サーバ前処理))

５－２　ＶＰＮＮＡＴ１１０解放コマンドを作成する。なお、リモートメンテナンス要求ＤＢ９２のテーブルレコードは図３１と同一である。

((コマンド送信処理))

５－３　保守サーバ３は、内線端末名をパラメータとして、保守サーバ３から端末１（ｈｔｔｐサーバ部１００）へのｈｔｔｐコマンドで＜ＩＰｓｅｃセッション＞としてＶＰＮＮＡＴ解放コマンドを送信する。

【０１９９】②ＶＰＮＮＡＴ解放コマンド受信処理（端末サーバ部１０→端末ルータ部１１）

((端末前処理))

５－４　端末サーバ部１０は、ＶＰＮＮＮＡＴ１１０解放コマンドを受信し、パラメータの内線端末２ａ～２ｎ名をキーとして、端末サーバ部１０がもっている端末名と実ＩＰアドレスの組のテーブル（ＤＮＳ等で参照）から端末名に対応する実ＩＰアドレスを取得する。

【０２００】そして、端末名に対応するＶＰＮＮＡＴ用

ローカルＩＰアドレスと実ＩＰアドレスのＶＰＮＮＡＴ１１０を解放するコマンド（複数の場合あり）（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる）を作成する。

【０２０１】((コマンド送信処理))

５－５　前の処理で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

((端末ルータ部処理))

５－６　ＶＰＮＮＡＴ１１０解放の設定をルータ部１１に書き込む。

【０２０２】((レスポンス送信処理))

５－７　ステータス（正常またはエラーステータス（コマンド異常等））をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

((端末ルータ設定部後処理))

５－８　ホストテーブルの端末名に対応するレコードを削除する。

【０２０３】③ＶＰＮＮＡＴ１１０解放レスポンス送信処理（端末サーバ部１０→保守サーバ３）

((レスポンス送信処理))

５－９　端末１のｈｔｔｐサーバ部１００は、ステータス（正常またはエラーステータス）をパラメータとし、端末１（サーバ部１０）から保守センタ９へのｈｔｔｐレスポンス＜ＩＰｓｅｃセッション＞としてレスポンスを送信する。

【０２０４】④保守サーバ側ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理（保守サーバ３）

((ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理))

５－１０　サーバ側で処理中の受付番号に対応する内線端末２ａ～２ｎに対応するＶＰＮＮＡＴ用ローカルＩＰアドレスをリモートメンテナンス要求ＤＢ９２から取得し、保持するとともに、ＶＰＮＮＡＴＤＢ９１の対応ＶＰＮＮＡＴ用ローカルＩＰアドレスを解放する。

【０２０５】⑤ＩＰｓｅｃ処理対象パケット解除設定（保守サーバ３→ＶＰＮゲートウェイ５）

((コマンド送信処理))

５－１１　ＶＰＮゲートウェイ設定処理部３２は、リモートメンテナンス要求ＤＢ９２の処理中の受付番号に該当するレコードから、端末ＩＤ、ＶＰＮＮＡＴ用ローカルＩＰアドレスを取得する。

【０２０６】５－１２　ＶＰＮゲートウェイ設定処理部３２は、ＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを端末ＩＤに対応したＶＰＮトンネル１２に割り付けるための設定を解除するためのコマンド（ＶＰＮゲートウェイ５のｔｅｌｎｅｔコマンドの実装により異なる）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。

【０２０７】((ＶＰＮゲートウェイ処理))

５－１３　受信したＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティングの設定をＶＰＮゲートウェイ５から解除する。

【０２０８】（レスポンス送信処理）

５－１４　ステータス（正常またはエラーステータス（コマンド異常等））をパラメータとして、ＶＰＮゲートウェイ５（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。

【０２０９】((ＶＰＮゲートウェイ設定処理部後処理))

５－１５　対応する情流ＧＷ端末１に対するリモートメンテナンスを全て終了したかを判断し、全て終了していたら、ＶＰＮ終了処理を起動し、全て終了していいなかったら、処理を終了する。

【０２１０】＜ＶＰＮ終了処理＞図９のシーケンス図及び図２３乃至図２５の手順フロー図に示すよう、ＶＰＮ終了処理は、リモートメンテナンス要求時に保守センタ９から構築されたＶＰＮを終了することを主旨とする。

【０２１１】①ＶＰＮ終了コマンド送信処理（保守サーバ３→端末サーバ部１０）

((通信契機))

６－１　ＶＰＮトンネル１２が張られている状態において、リモートメンテナンス終了後、対応する情流ＧＷ端末１に対するメンテナンスが全て終了した場合に起動される。

【０２１２】((サーバ前処理))

６－２　ＶＰＮ終了コマンドを作成する。なお、リモートメンテナンス要求ＤＢ９２のテーブルレコードは図２９と同一である。

（コマンド送信処理）

６－３　保守サーバ３は、保守サーバ３から端末１（ｈｔｔｐサーバ部１００）へのｈｔｔｐコマンドで＜ＩＰｓｅｃセッション＞としてＶＰＮ終了コマンドを送信する。

【０２１３】②ＶＰＮ終了コマンド受信処理（端末サーバ部１０→端末ルータ部１１）

((端末前処理))

６－４　端末サーバ部１０は、ＶＰＮ終了コマンドを受信し、全てのＶＰＮＮＡＴ１１０を解放するコマンド（複数の場合あり）（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる）を作成する。

【０２１４】((コマンド送信処理))

６－５　前の処理で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ル

ータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。
③ＶＰＮＮＡＴ設定初期化コマンド受信及び処理（ルータ部１１）
((端末ルータ部処理))
６－６　ＶＰＮＮＡＴ１１０解放の設定をルータ部１１に書き込む。
【０２１５】((レスポンス送信処理))
６－７　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜ローカルセッション＞としてレスポンスを送信する。
((端末ルータ設定部後処理))
６－８　ホストテーブルを全て削除する。
【０２１６】④ＶＰＮ終了レスポンス送信処理（端末サーバ部１０→保守サーバ１１）
((レスポンス送信処理))
６－９　端末１のｈｔｔｐサーバ部１００は、ステータス（正常またはエラーステータス）をパラメータとし、端末１（ｈｔｔｐサーバ部１００）から保守センタ９へのｈｔｔｐレスポンス＜ＩＰｓｅｃセッション＞としてレスポンスを送信する。
【０２１７】⑤保守サーバ側ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理（保守サーバ３）
((ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理))
６－１０　サーバ側で処理中の受付番号に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスを全てリモートメンテナンス要求ＤＢ９２から取得し、保持するとともに、ＶＰＮＮＡＴＤＢ９１の対応ＶＰＮＮＡＴ用ローカルＩＰアドレスを解放する。
【０２１８】⑥ＩＰＳｅｃ処理対象パケット解除設定（保守サーバ３→ＶＰＮゲートウェイ５）
((コマンド送信処理))
６－１１　ＶＰＮゲートウェイ設定処理部３２は、リモートメンテナンス要求ＤＢ９２の該当レコードから、端末ＩＤに対応するすべての端末ＩＤ、ＶＰＮＮＡＴ用ローカルＩＰアドレスを取得する。
【０２１９】６－１２　ＶＰＮゲートウェイ設定処理部３２は、ＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを端末ＩＤに対応したＶＰＮトンネル１２に割り付けるための設定を解除するためのコマンド（ＶＰＮゲートウェイ５のｔｅｌｎｅｔコマンドの実装により異なる）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。
【０２２０】((ＶＰＮゲートウェイ処理))
６－１３　受信したＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティングの設定をＶＰＮゲートウェイ５ｉから解除する。
【０２２１】((レスポンス送信処理))
６－１４　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、ＶＰＮゲートウェイ５（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。
【０２２２】⑦ＩＰｓｅｃ設定解除コマンド送信処理（保守サーバ３→ＶＰＮゲートウェイ５）
((コマンド送信処理))
６－１５　ＶＰＮゲートウェイ設定処理部３２は、処理中の受付番号に対応するリモートメンテナンス要求ＤＢ９２のレコードから、端末ＩＤを取得する。
【０２２３】６－１６　ＶＰＮゲートウェイ設定処理部３２は、端末ＩＤに対応したＶＰＮトンネル１２を解除するための設定（ＶＰＮゲートウェイ５のｔｅｌｎｅｔコマンドの実装により異なる）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。
【０２２４】⑧ＩＰｓｅｃ設定解除コマンド受信及び処理（ＶＰＮゲートウェイ５）
((ＶＰＮゲートウェイ処理))
６－１７　受信した端末ＩＤに対応するＶＰＮの設定をＶＰＮゲートウェイ５から解除する。
【０２２５】((レスポンス送信処理))
６－１８　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、ＶＰＮゲートウェイ５（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。
【０２２６】((ＶＰＮゲートウェイ設定処理部後処理))
６－１９　ＶＰＮＧＷアドレス要求処理でＶＰＮゲートウェイトンネルＤＢから取得保持し「端末ＩＤ」を書き込んだフィールドを「未使用」に書き換え、ＶＰＮトンネルリソースを解放する。
上記でリモートメンテナンス終了処理が完了となる。以上、シーケンス図３～シーケンス図９及び手順フロー図１３～手順フロー図２５をもとに、リモートメンテナンスの処理手順を説明した。
【０２２７】本記録媒体例は、当該リモートメンテナンスの処理プログラム手順の一連の完結手続をコンピュータ読取り自在に実録したものである。
【０２２８】本実施形態例では、情流ＧＷ端末１本体のサーバ部１０及びルータ部１１へのＶＰＮＮＡＴ１１０の設定は設置通知時に行っているが、これはリモートメ

ンテナンス要求なしに、保守センタ９側から任意の契機で情流ＧＷ端末１にＶＰＮアクセスを可能とするための機能である。したがって、情流ＧＷ端末１本体のサーバ部１０及びルータ部１１へのＶＰＮＮＡＴ１１０の設定を特別扱いせずに、リモートメンテナンス要求時にＶＰＮＮＡＴ１１０を設定し、それをＶＰＮＮＡＴ１１０解放時に解放する手順でもよいのは言うまでもない。

【０２２９】本実施例においては、ＶＰＮにＩＰｓｅｃを用いて説明しているが、本発明はレイヤ３レベルのＶＰＮであればＩＰｓｅｃ以外に対しても適用可能なことは言うまでもない。

【０２３０】

【発明の効果】かくして、本発明によれば、ＶＰＮＮＡＴに用いる有限のＶＰＮＮＡＴ用ローカルＩＰアドレスリソースが、リモートメンテナンス要求端末に対してだけ割り当てられて、リモートナンス終了時にＶＰＮＮＡＴ解放プロセスで解放されることにより、ＩＰアドレス資源が節約でき、静的ＶＰＮＮＡＴ方式と比較して同時に多くの端末をリモートメンテナンスできる。

【０２３１】言い換えれば、従来は最大「ＶＰＮＮＡＴ用ローカルＩＰアドレスリソース」分の内線端末をリモートメンテナンス対象端末となっていたのに対し、本発明を用いることにより、同時に「ＶＰＮＮＡＴ用ローカルＩＰアドレスリソース」分の内線端末をリモートメンテナンス対象端末とすることが可能になり、リモートメンテナンスサービス対象端末の加入者数を大幅に増やすことができる。

【０２３２】しかも、ＶＰＮＮＡＴに用いる有限のＶＰＮＮＡＴ用ローカルＩＰアドレスリソースが、リモートメンテナンス要求端末に対してだけ割り当てられて、リモートナンス終了時にＶＰＮＮＡＴ解放プロセスで解放されることにより、リモートメンテナンス要求対象とした内線端末に対してだけ保守センタからのアクセスを許すリモートメンテナンス方法を実現することができる。

【０２３３】また、リモートメンテナンスサービス提供者にとっては、保守センタがＶＰＮゲートウェイの設備を設置する際、ＶＰＮリモートメンテナンスのアクセス数に応じてＶＰＮゲートウェイの設備を増設設置することができ、ひいては、ＶＰＮゲートウェイの設備コストを最適化できる。

【０２３４】前述の効果から、リモートメンテナンスサービスを享受するお客様にとっては、保守センタとＶＰＮを構築する際ＶＰＮのリソース不足となることが少なくなり、ＶＰＮ構築失敗でリモートメンテナンスを受けられなくなるケースが減少する。

【図面の簡単な説明】

【図１】本発明の実施の形態を示すシステム例のシステム構成図である。

【図２】同上において、ＶＰＮＮＡＴに動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与する機能説明図である。

【図３】本発明の実施の形態を示す方法例における設置通知処理のシーケンス図である。

【図４】同上におけるＶＰＮＧＷアドレス要求処理のシーケンス図である。

【図５】同上におけるリモートメンテナンス要求処理のシーケンス図である。

【図６】同上におけるリモートメンテナンス実施処理のシーケンス図である。

【図７】同上におけるリモートメンテナンス終了処理のシーケンス図である。

【図８】同上におけるＶＰＮＮＡＴ解放処理のシーケンス図である。

【図９】同上におけるＶＰＮ終了処理のシーケンス図である。

【図１０】本発明の実施の形態を示すプログラム例及び記録媒体例における情報ＧＷ端末側概括フローチャートである。

【図１１】同上における保守センタ側概括フローチャートである。

【図１２】同上における設置通知処理の前半フロー手順図である。

【図１３】同上における設置通知処理の後半フロー手順図である。

【図１４】同上におけるＶＰＮＧＷアドレス要求処理の前半フロー手順図である。

【図１５】同上におけるＶＰＮＧＷアドレス要求処理の後半フロー手順図である。

【図１６】同上におけるリモートメンテナンス要求処理の初期段階フロー手順図である。

【図１７】同上におけるリモートメンテナンス要求処理の第２段階フロー手順である。

【図１８】同上におけるリモートメンテナンス要求処理の最終段階フロー手順図である。

【図１９】同上におけるリモートメンテナンス実施処理のフロー手順図である。

【図２０】同上におけるリモートメンテナンス終了処理のフロー手順図である。

【図２１】同上におけるＶＰＮＮＡＴ解放処理の前半フロー手順図である。

【図２２】同上におけるＶＰＮＮＡＴ解放処理の後半フロー手順図である。

【図２３】同上におけるＶＰＮ終了処理の初期フロー手順図である。

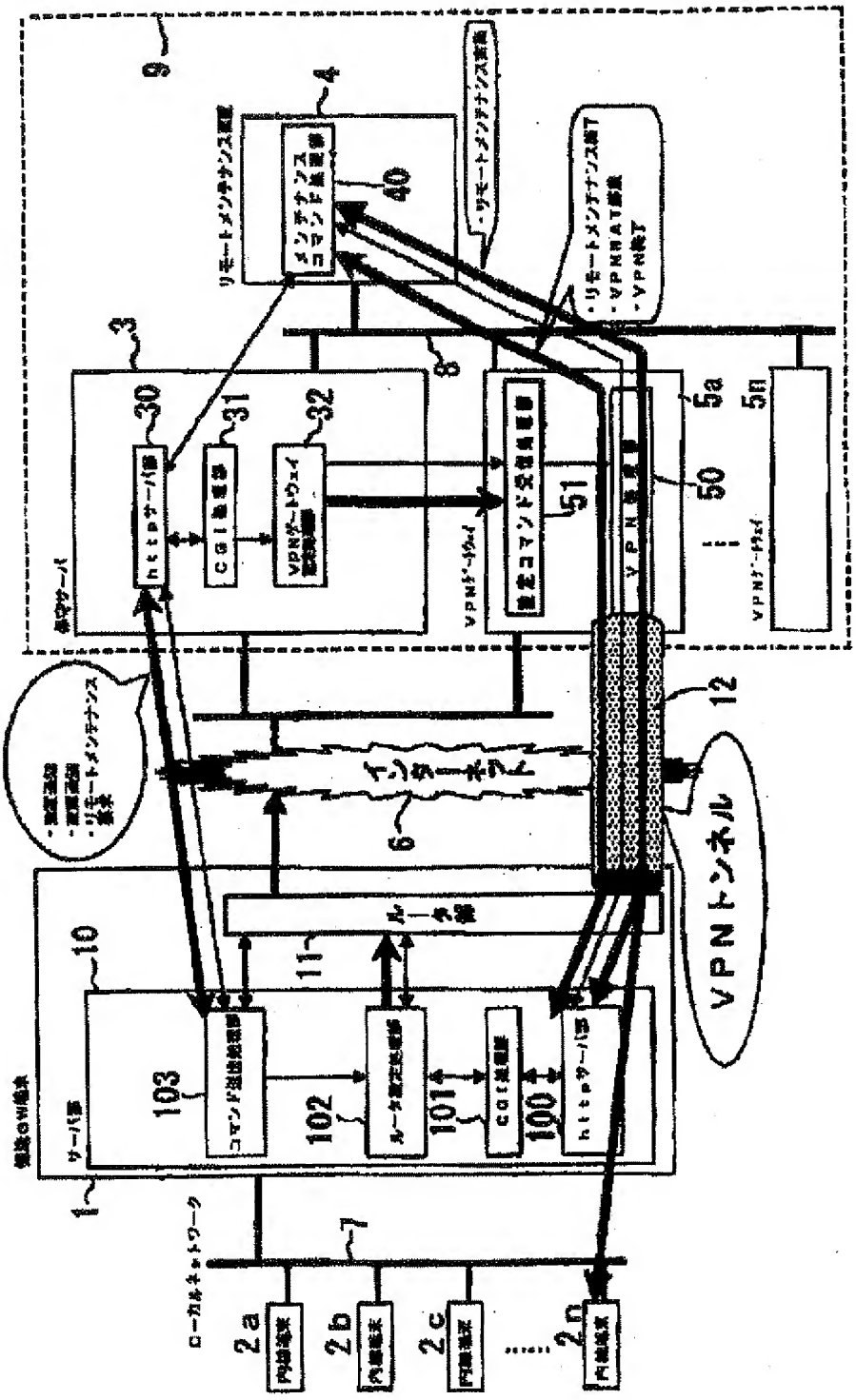
【図２４】同上におけるＶＰＮ終了処理の中間フロー手順図である。

【図２５】同上におけるＶＰＮ終了処理の最終フロー手順図である。

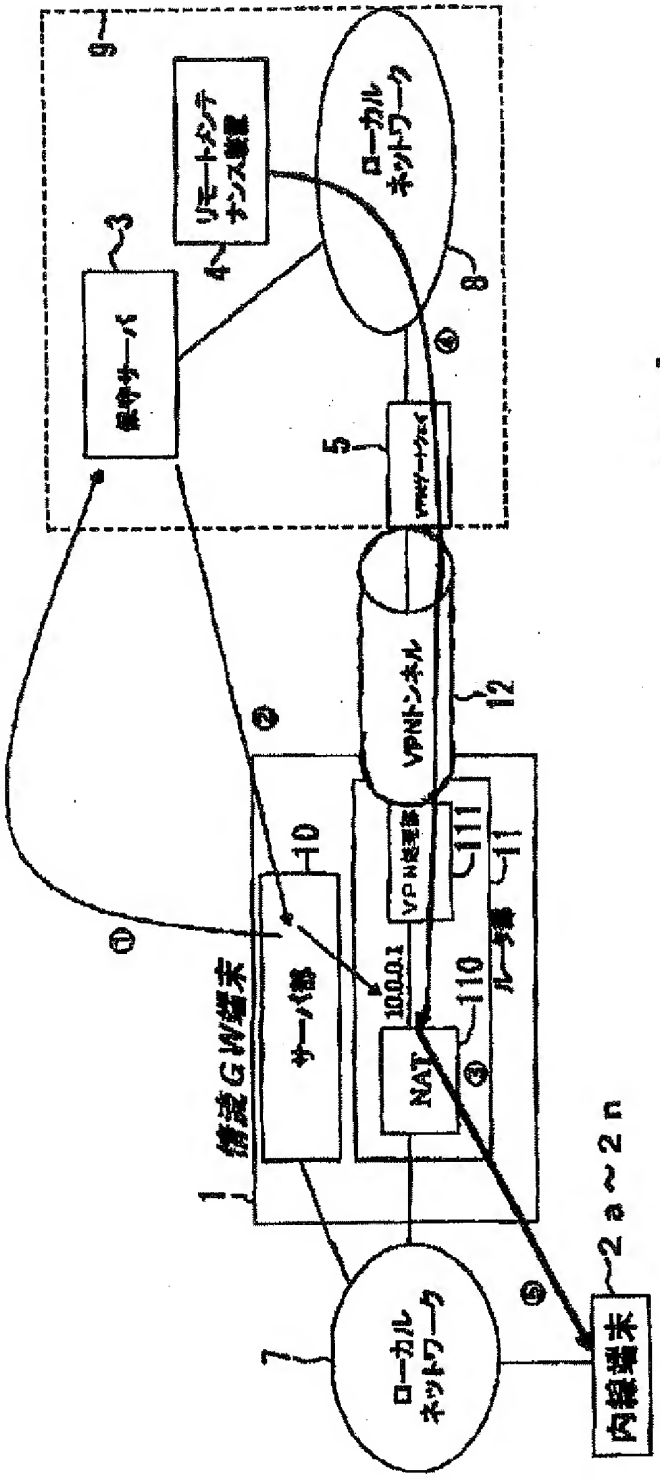
【図２６】本発明の実施の形態を示す方法例における故障通知処理のシーケンス図である。

【図２７】本発明の実施の形態を示すプログラム例及び記録媒体例における故障通知処理のフロー手順図である。
【図２８】図１６中、端末ＤＢ９０のレコード内容を示すテーブルである。
【図２９】図１６中、リモートメンテナンス要求ＤＢ９２のレコード内容を示すテーブルである。
【図３０】図１６中、ＶＰＮＮＡＴＤＢ９１のレコード内容を示すテーブルである。
【図３１】図２０中、リモートメンテナンス要求ＤＢ９２のレコード内容を示すテーブルである。
【図３２】従来システムにおけるＶＰＮＮＡＴの機能説明図である。
【図３３】同上における２地点同時接続のＶＰＮＮＡＴの機能説明図である。
【符号の説明】
１…インターネットゲートウェイ端末（端末情流ＧＷ端末）
２ａ～２ｎ…内線端末
３…保守サーバ
４…リモートメンテナンス装置
５、５ａ、５ｉ、５ｎ…ＶＰＮゲートウェイ（ＶＰＮＧＷ）
６…インターネット
７，８…ローカルネットワーク（ＬＡＮ）
９…保守センタ（センタ）
１０…サーバ部（端末サーバ部）
１１…ルータ部（端末ルータ部、ＶＰＮルータ部）
１２…ＶＰＮトンネル
３０，１００…ｈｔｔｐサーバ部
３１，１０１…ＣＧＩ処理部
３２…ＶＰＮゲートウェイ設定処理部
４０…メンテナンスコマンド処理部
５０…ＶＰＮ処理部
５１…設定コマンド受信処理部
１０２…ルータ設定処理部
１０３…コマンド送出処理部
１１０…ＮＡＴ（ＶＰＮＮＡＴ）

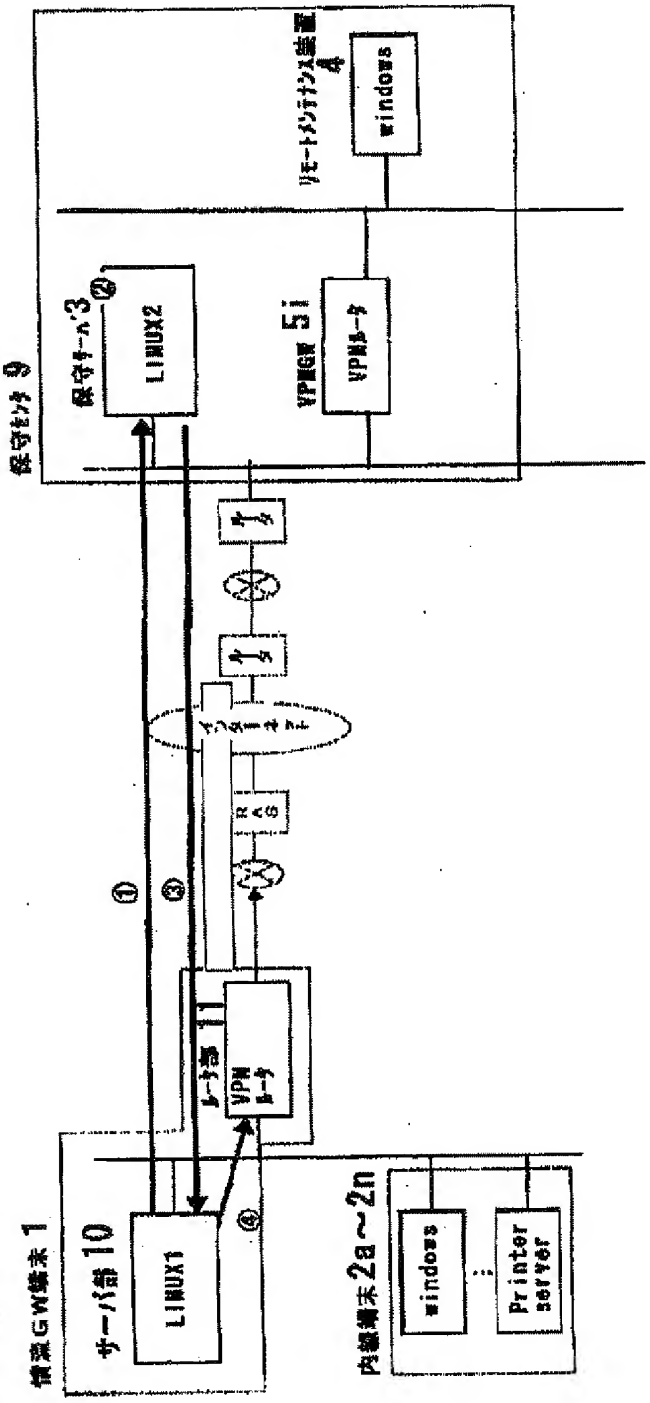
【図1】


9
4
40
3
30
31
32
8
5a
5n
50
51
12
VPNトンネル
6
10
11
103
102
101
100
1
7
2a
2b
2c
2n

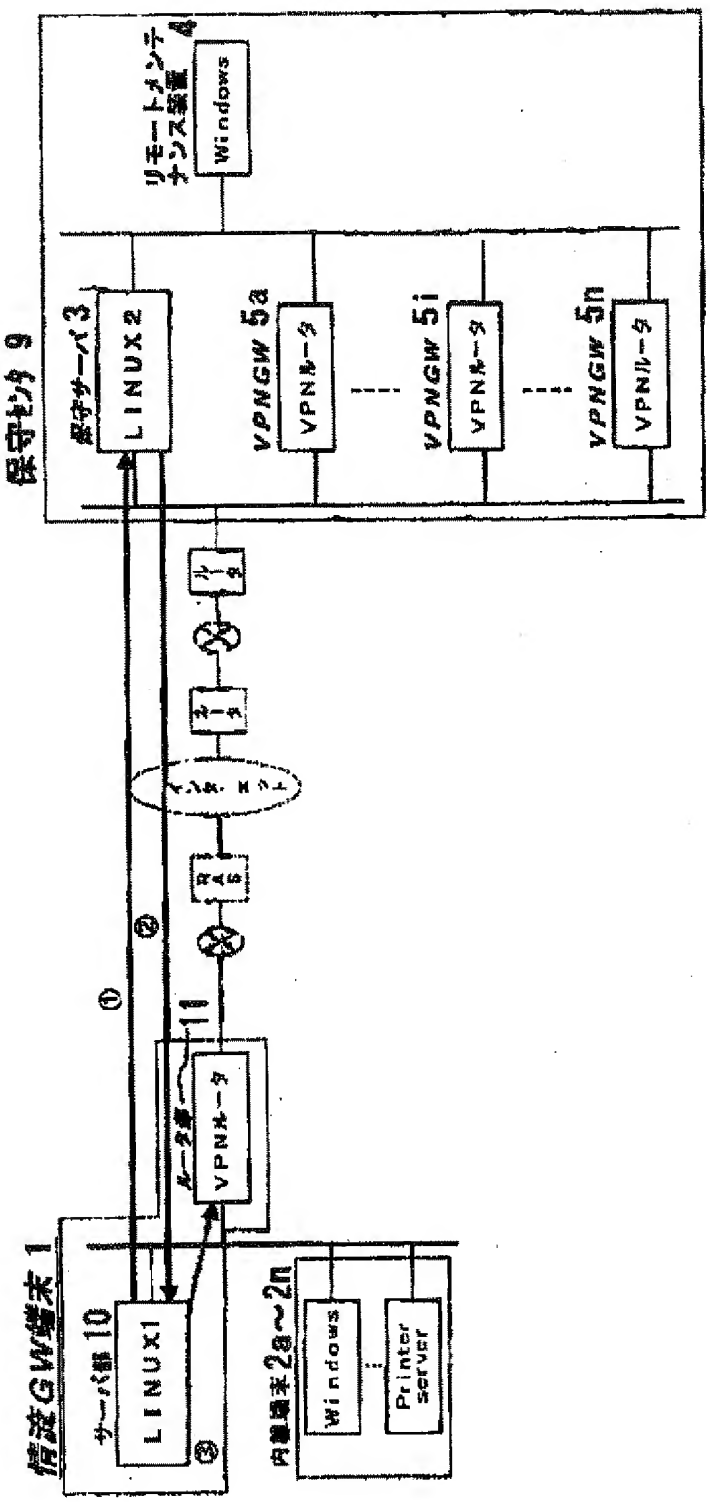
【図2】


9
リモートメンテナンス装置
4
ローカルネットワーク
8
保守サーバ
3
5
VPNトンネル
12
10
VPN処理部
111
11
10.0.0.1
110
NAT
ルータ部
情報GW端末
1
サーバ部
ローカルネットワーク
7
内線端末
2a～2n

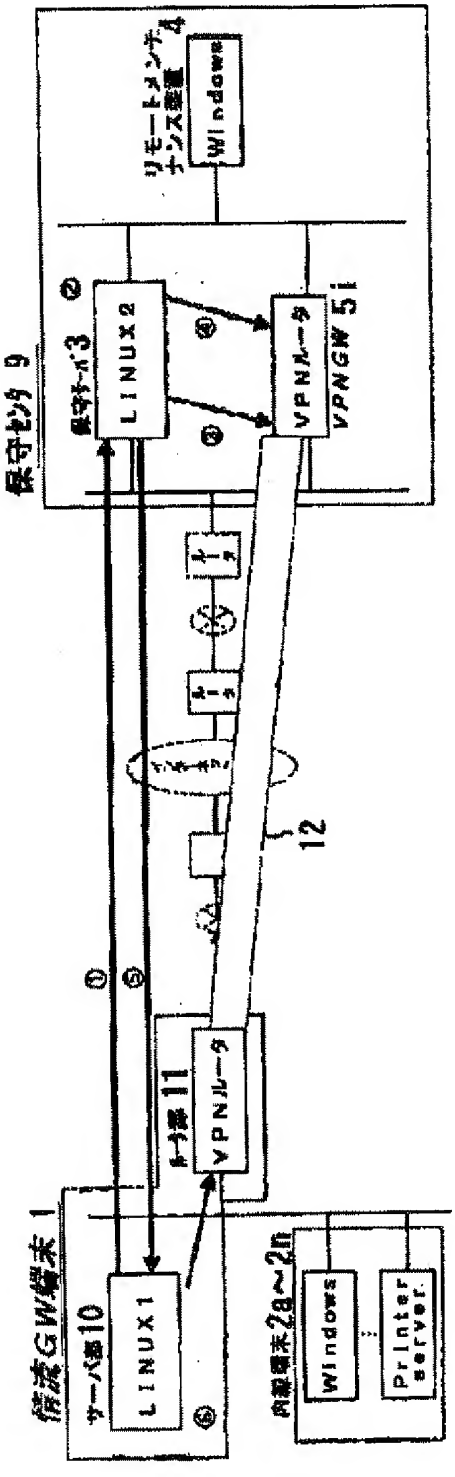
【図4】


保守セット 9
保守サーバ 3
LINUX2
VPNGW 5i
VPNルータ
リモートメンテナンス装置 4
windows
インターネット
RAS
VPN ルータ
ルータ部 11
情報GW端末 1
サーバ部 10
LINUX1
内線端末2a～2n
windows
Printer server

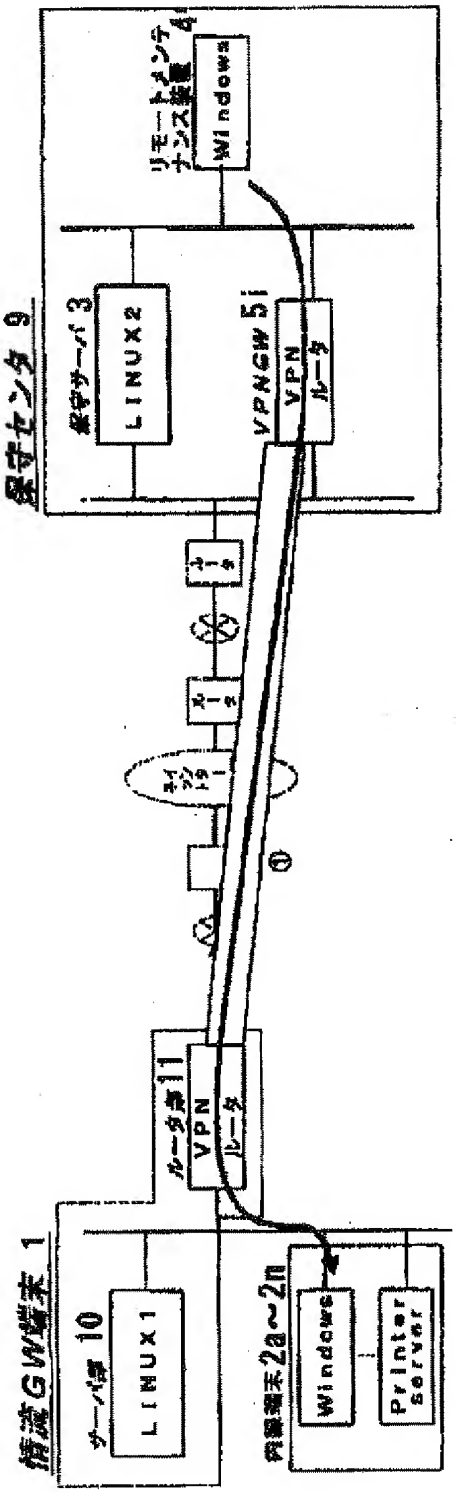
【図3】


保守センタ 9
リモートメンテナンス装置 4
Windows
保守サーバ 3
LINUX2
VPNGW 5a
VPNGW 5i
VPNGW 5n
VPNルータ
ルータ
ファイアウォール
RAS
11
VPNルータ
信濃GW端末 1
サーバ群 10
LINUX1
内線端末 2a～2n
Windows
Printer server
①
②
③

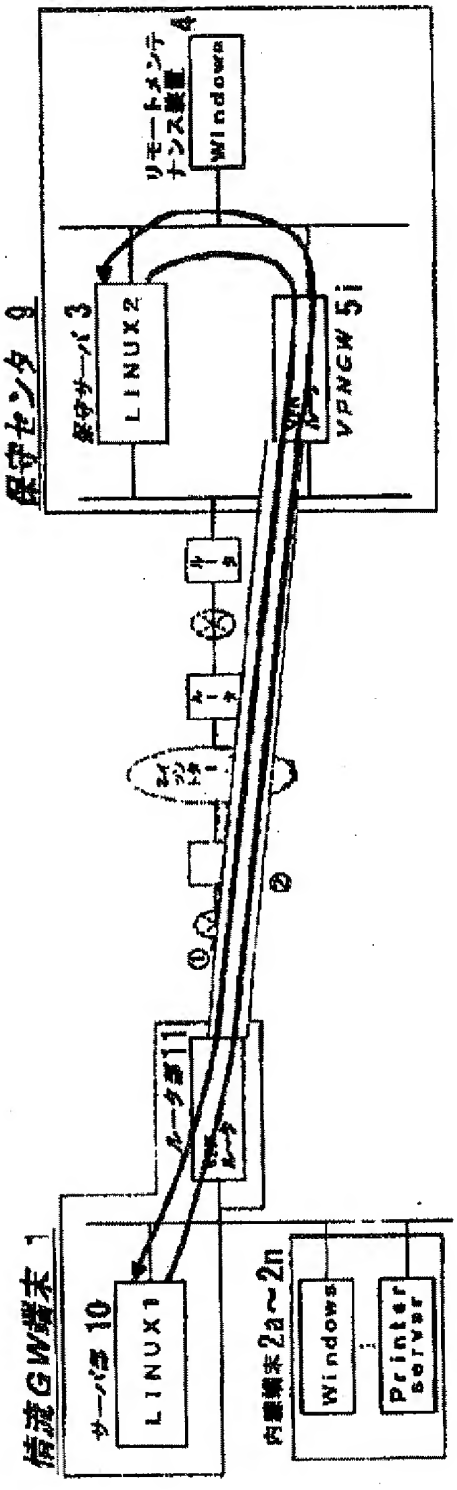
【図5】


保守センタ 9
リモートメンテナンス装置 4
Windows
保守サーバ 3
LINUX2
VPNGW 5i
VPNルータ
ルータ
ファイアウォール
12
11
VPNルータ
信濃GW端末 1
サーバ群 10
LINUX1
内線端末 2a～2n
Windows
Printer server
①
②
③
④
⑤
⑥

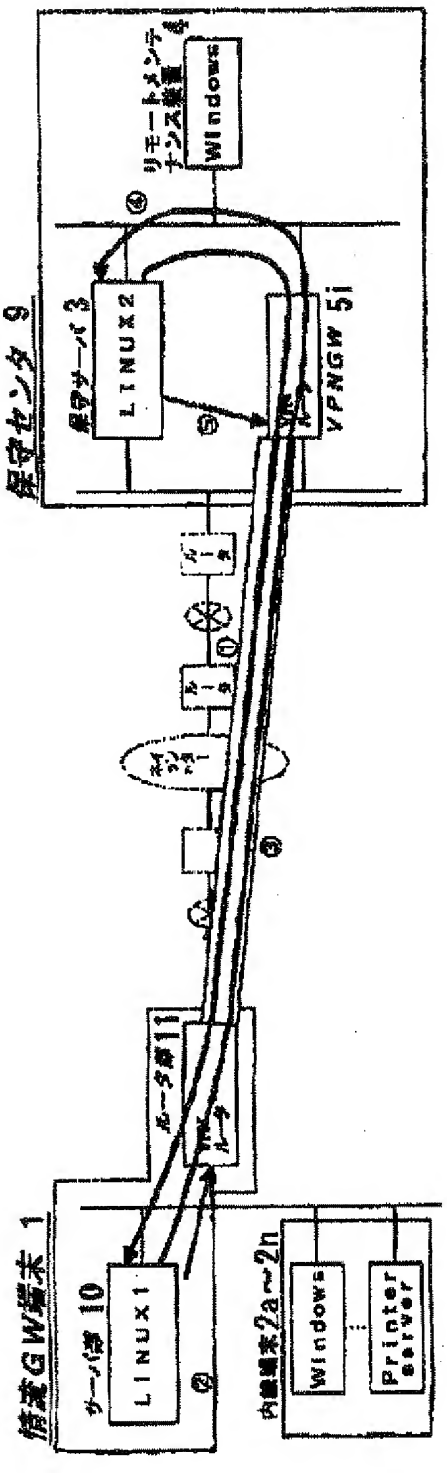
【図６】


保守センタ 9
保守サーバ 3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
VPN ルータ
ルータ
ファイアウォール
ルータ部 11
VPN ルータ
情流GW端末 1
サーバ部 10
LINUX1
内部端末 2a～2n
Windows
Printer server
①
②

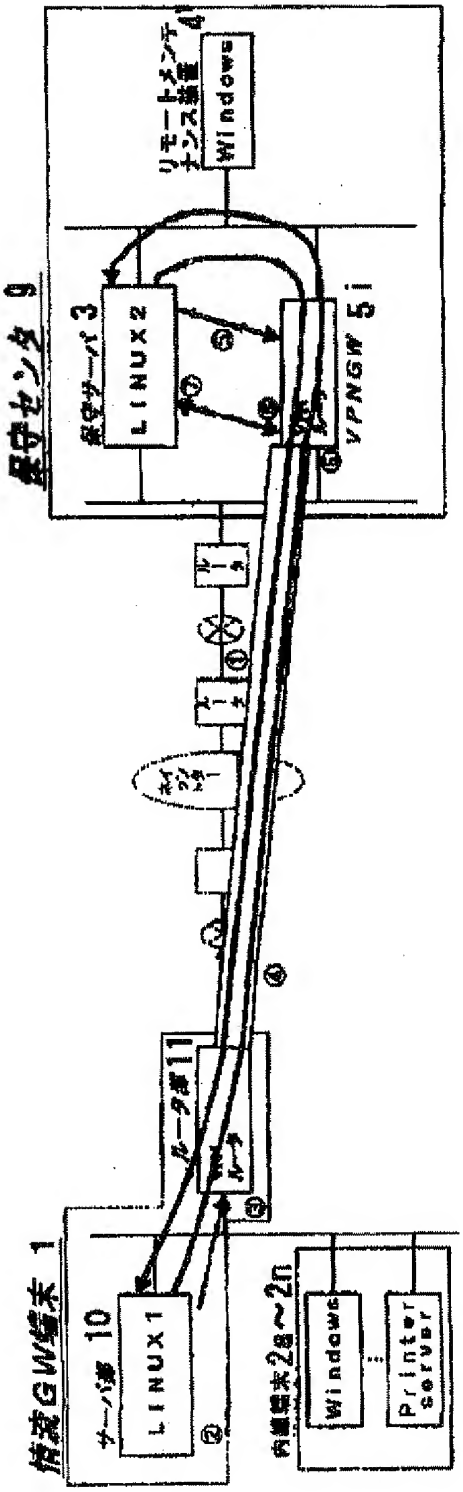
【図７】


保守センタ 9
保守サーバ 3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
ルータ
ファイアウォール
ルータ部 11
情流GW端末 1
サーバ部 10
LINUX1
内部端末 2a～2n
Windows
Printer server
①
②

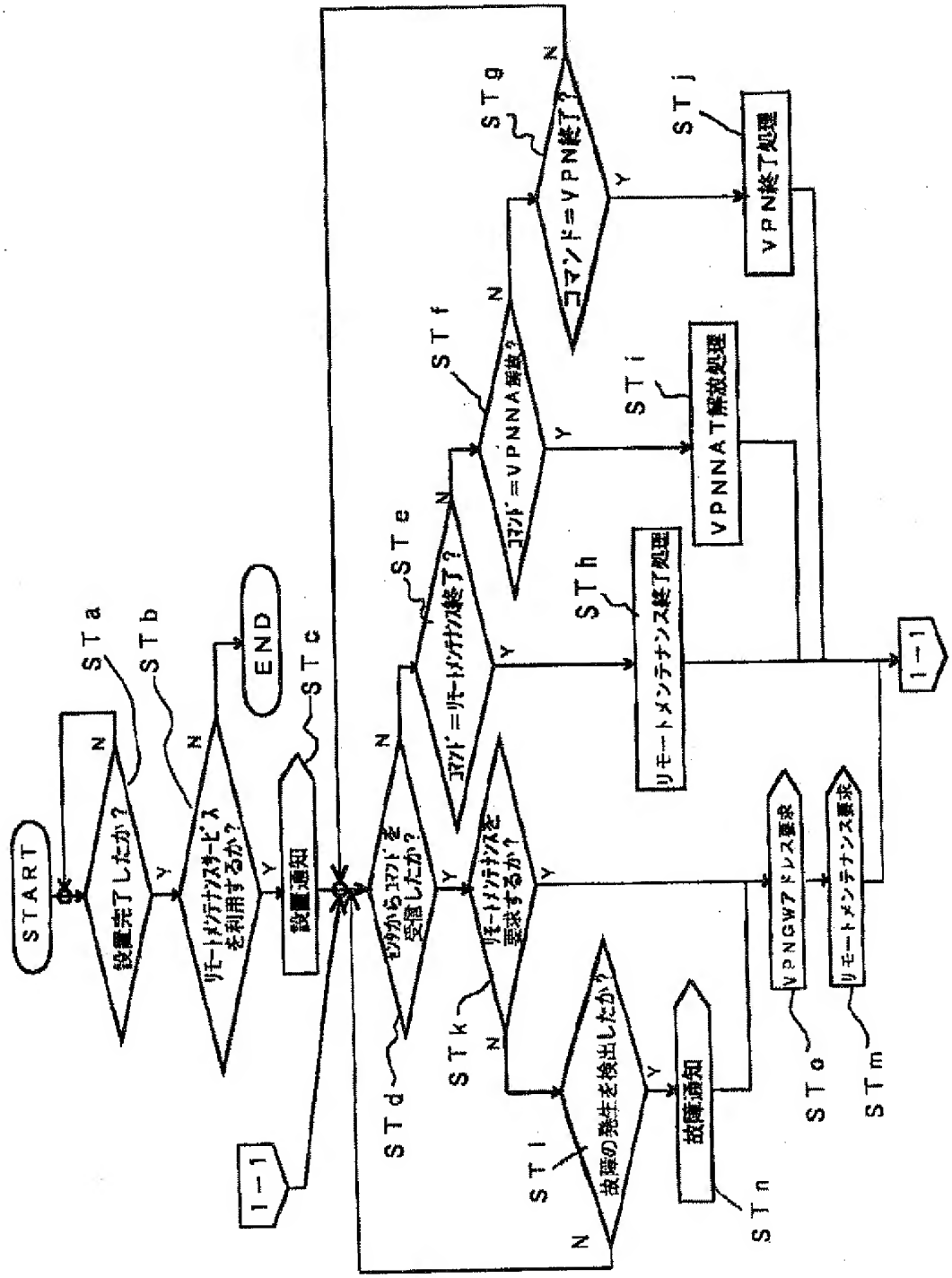
【図８】


保守センタ 9
保守サーバ 3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
情流GW端末 1
サーバ部 10
LINUX1
ルータ部 11
ルータ
内線端末2a～2n
Windows
Printer server

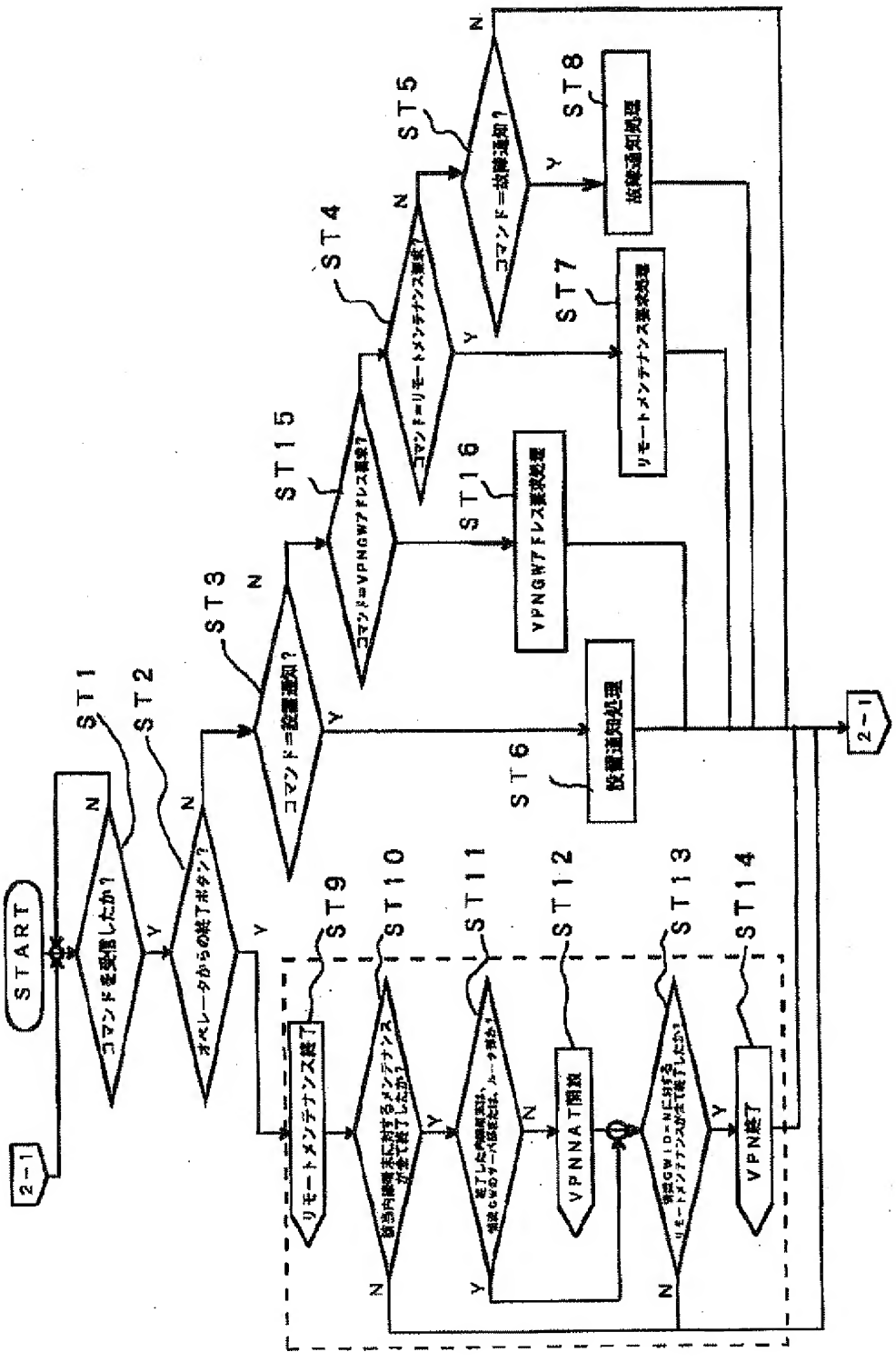
【図９】


保守センタ 9
保守サーバ 3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
情流GW端末 1
サーバ部 10
LINUX1
ルータ部 11
ルータ
内線端末2a～2n
Windows
Printer server

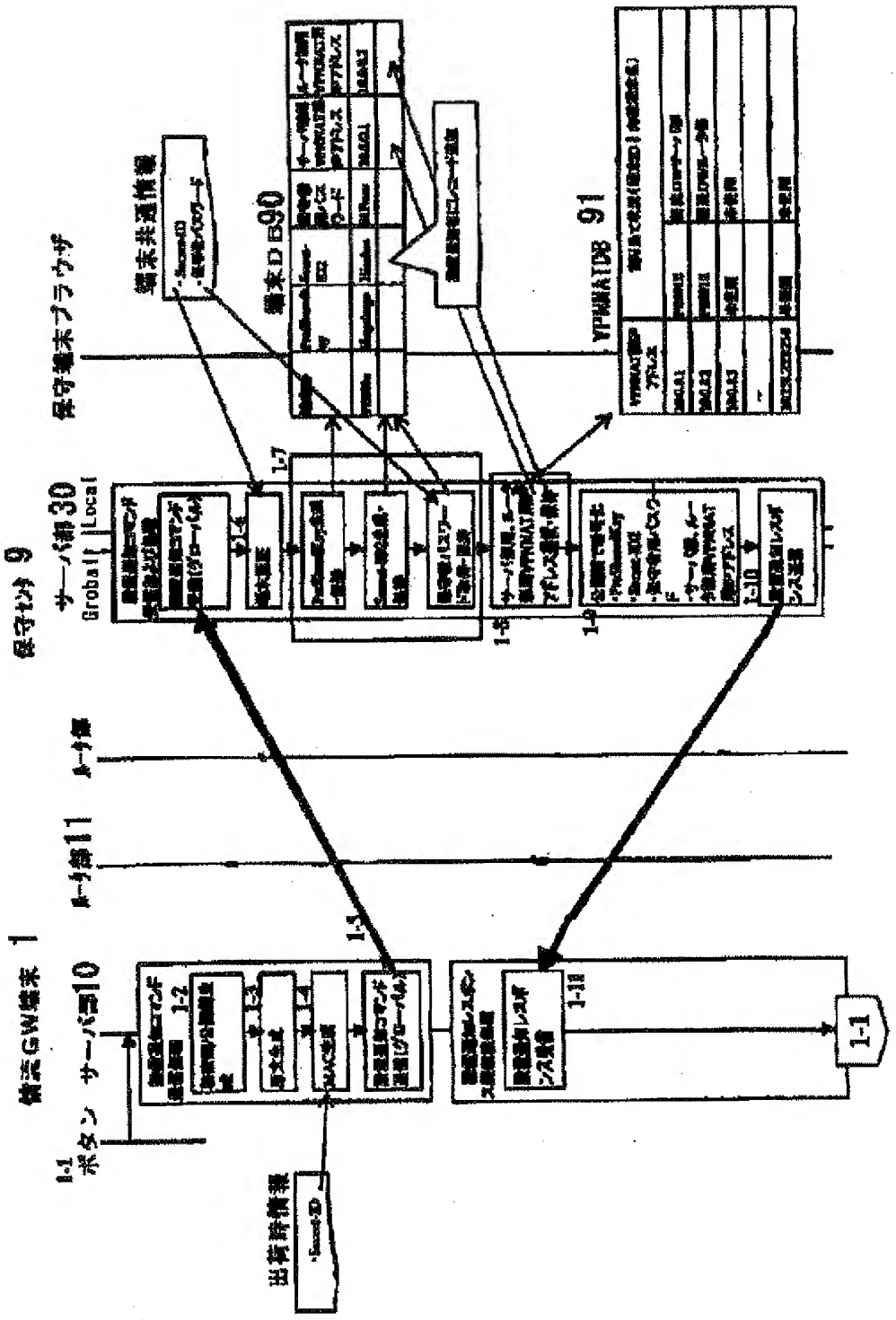
【図１０】


START
設置完了したか？
ST a
N
Y
ST b
リモートメンテナンスオーピスを利用するか？
N
Y
END
設置通知
ST c
1－1
ST d
モデムからコマンドを受信したか？
N
Y
ST e
コマンド＝リモートメンテナンス終了？
N
Y
ST f
コマンド＝VPNNA解放？
N
Y
ST g
コマンド＝VPN終了？
N
Y
ST h
リモートメンテナンス終了処理
ST i
VPNNAT解放処理
ST j
VPN終了処理
1－1
ST k
リモートメンテナンスを要求するか？
N
Y
ST l
故障の発生を検出したか？
N
Y
故障通知
ST n
VPNGWアドレス要求
ST o
リモートメンテナンス要求
ST m

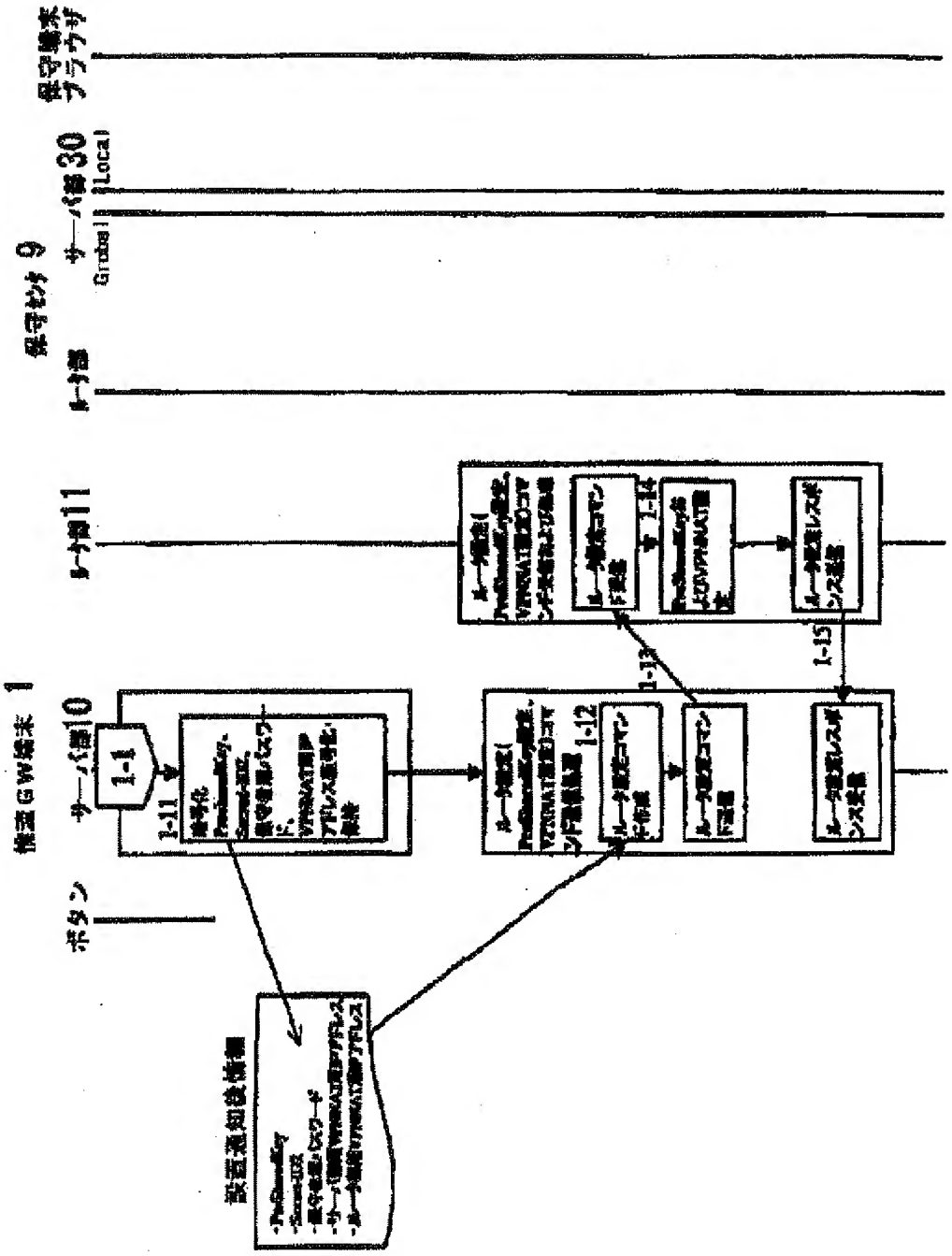
【図１１】


START
2－1
ST1
コマンドを受信したか?
N
Y
ST2
オペレータからの終了ボタン?
N
Y
ST3
コマンド＝故障通知?
N
Y
ST15
コマンド＝VPNGWアドレス要求?
N
Y
ST4
コマンド＝リモートメンテナンス要求?
N
Y
ST5
コマンド＝故障通知?
N
Y
ST8
故障通知処理
ST7
リモートメンテナンス要求処理
ST16
VPNGWアドレス要求処理
ST6
故障通知処理
2－1
ST9
リモートメンテナンス終了
ST10
ST11
ST12
VPNNAT開放
ST13
ST14
VPN終了

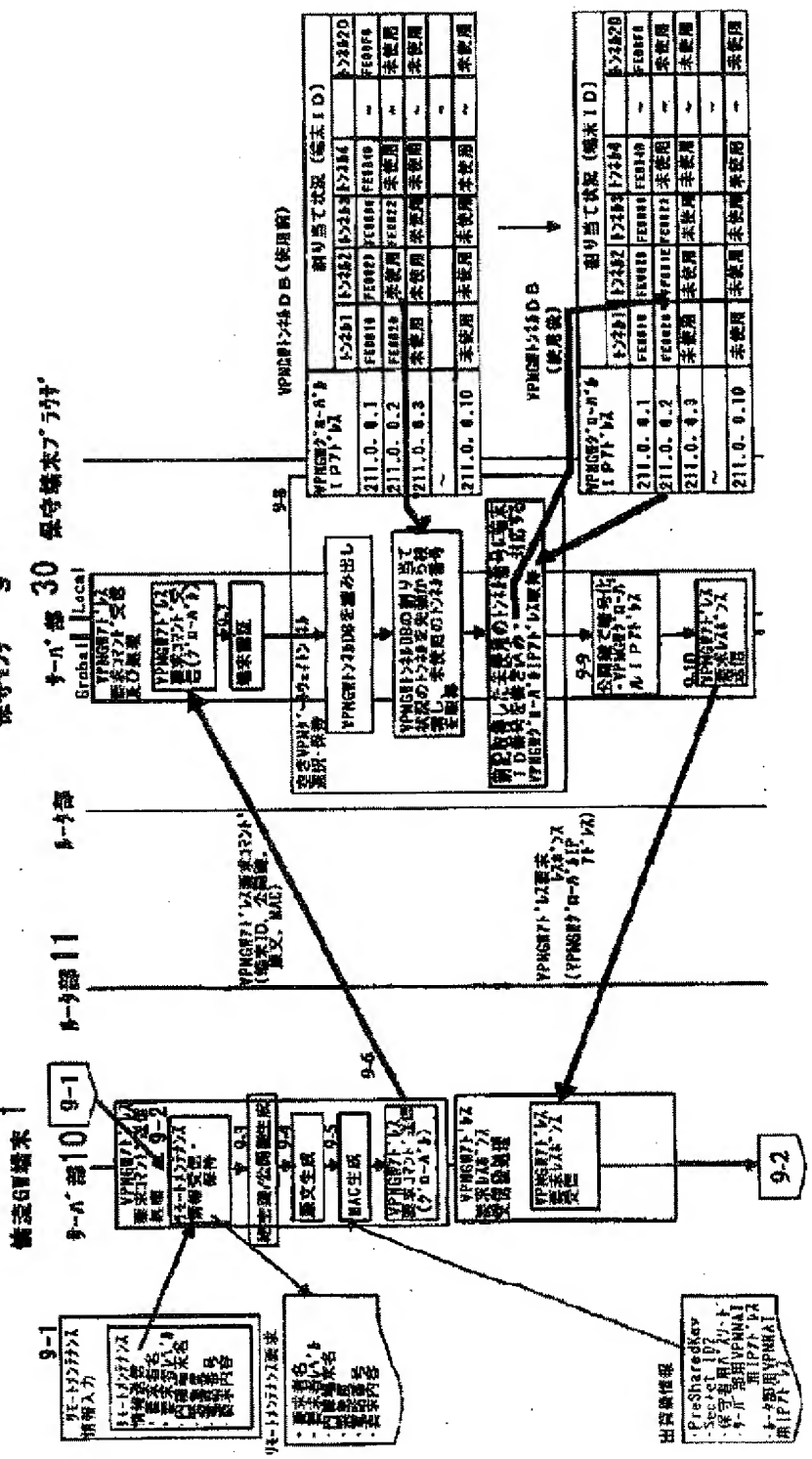
【図１２】


保守端末ブラウザ
端末共通情報
端末DB 90
VPN端末DB 91
保守センタ 9
サーバ群 30
Global
Local
ルータ群 11
サーバ群 10
端末GW端末 1
ボタン
出荷時情報
1-1

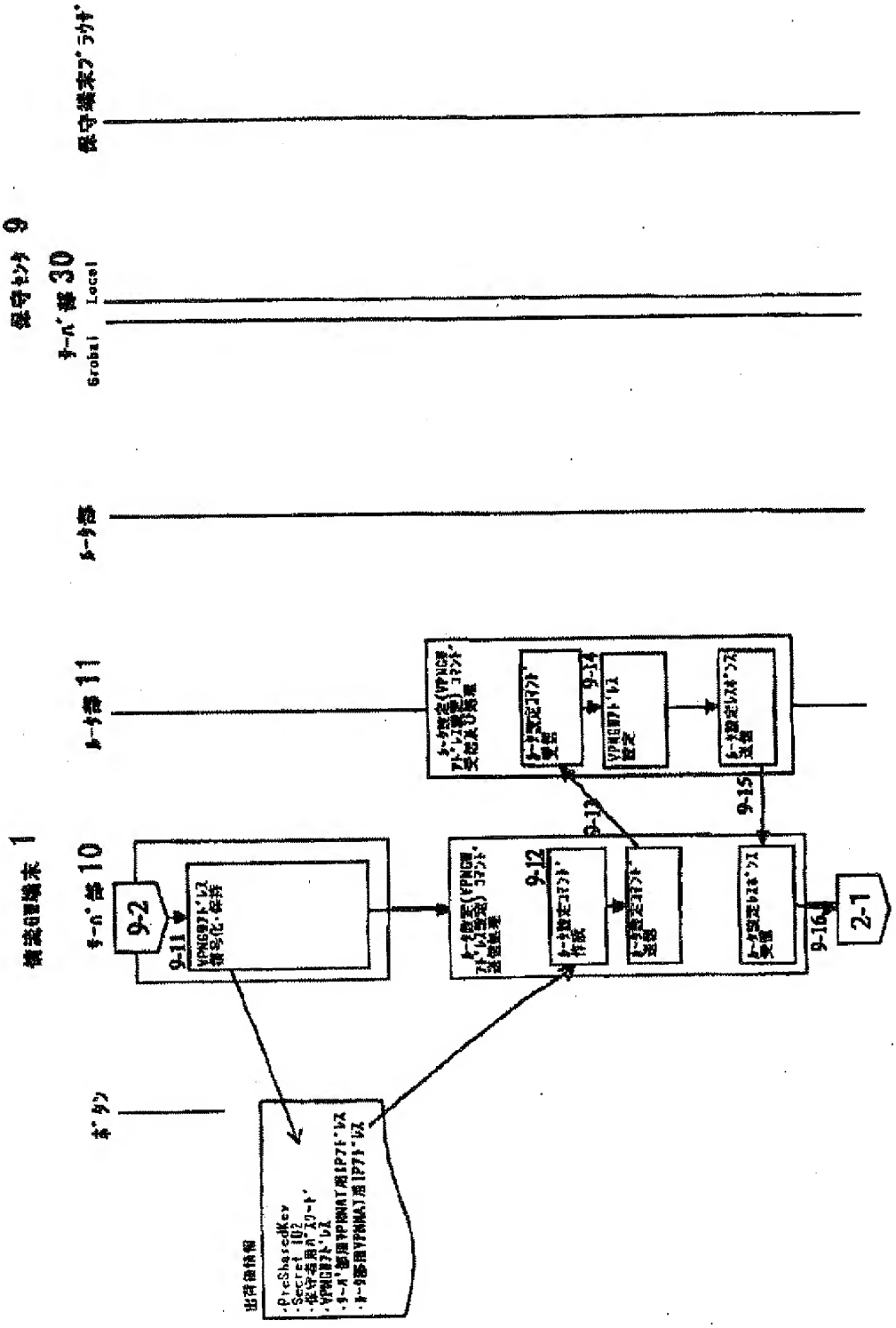
【図１３】


保守端末
ブラウザ
保守セット 9
サーバ部 30
Global
Local
ルータ部
ルータ部11
1-14
1-15
1-13
1-12
1-11
1-1
サーバ部10
無線GW装置 1
ボタン
設置通知後情報

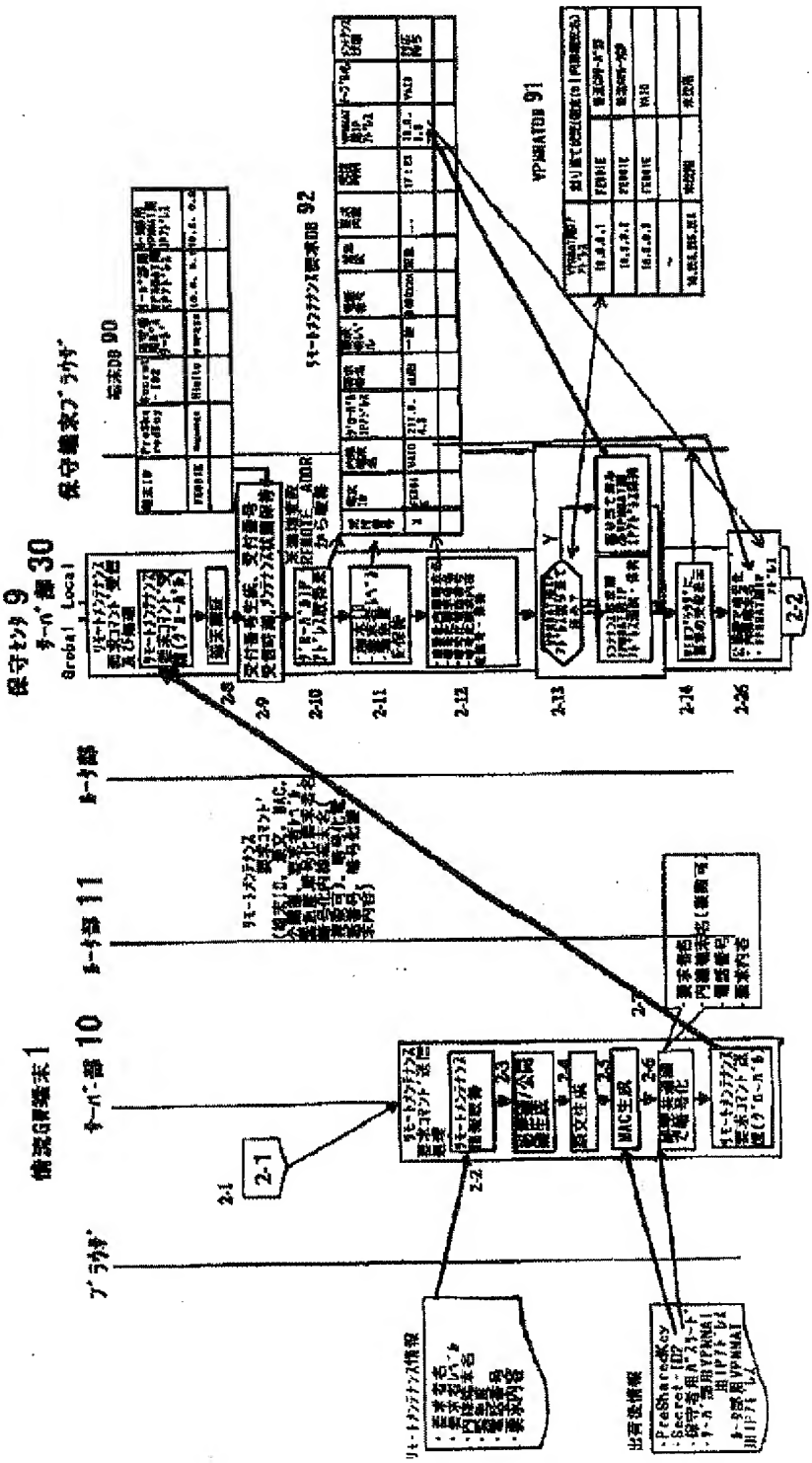
【図１４】


保守センタ
9
ルータ部
30
保守端末プラザ
ルータ部
11
ルータ部
10
接続自宅端末
1
9-1
9-2
9-3
9-4
9-5
9-6
9-7
9-8
9-9
9-10
VPN割当ｼｽﾃﾑDB（使用前）
VPN割当ｼｽﾃﾑDB
（使用後）
割り当て状況（端末ＩＤ）
未使用
出資情報

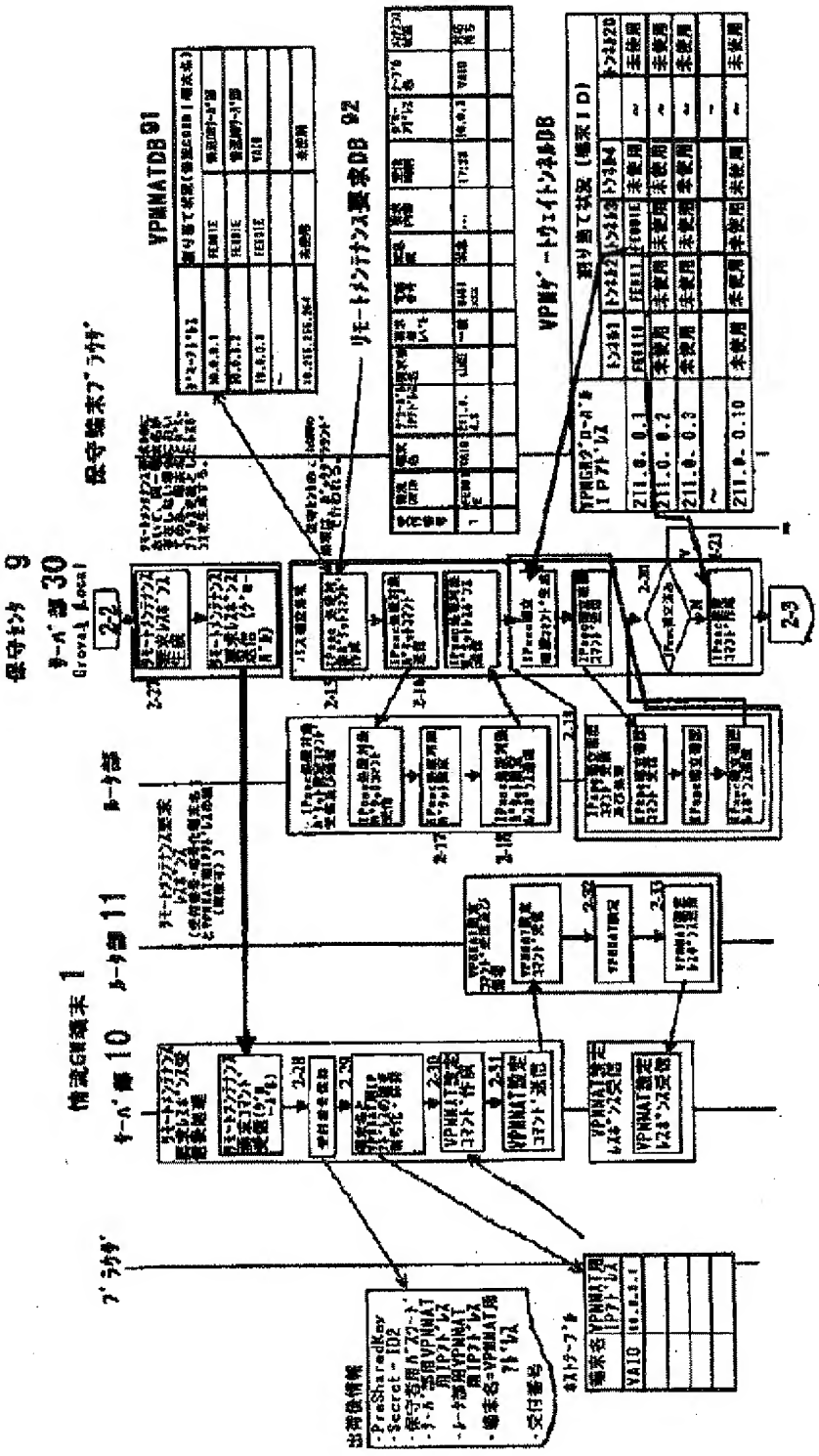
【図１５】


保守センタ 9
ルータ部 30
Global
Local
保守端末プログラム
ルータ部
ルータ部 11
端末管理端末 1
ルータ部 10
9-2
9-11
9-12
9-13
9-14
9-15
9-16
2-1
ポリシ
出荷時情報
・PreSharedKey
・Secret ID2
・保守者用ID/PW
・VPN用ID/PW
・ルータ1号機VPN/NAT用IPアドレス
・ルータ2号機VPN/NAT用IPアドレス

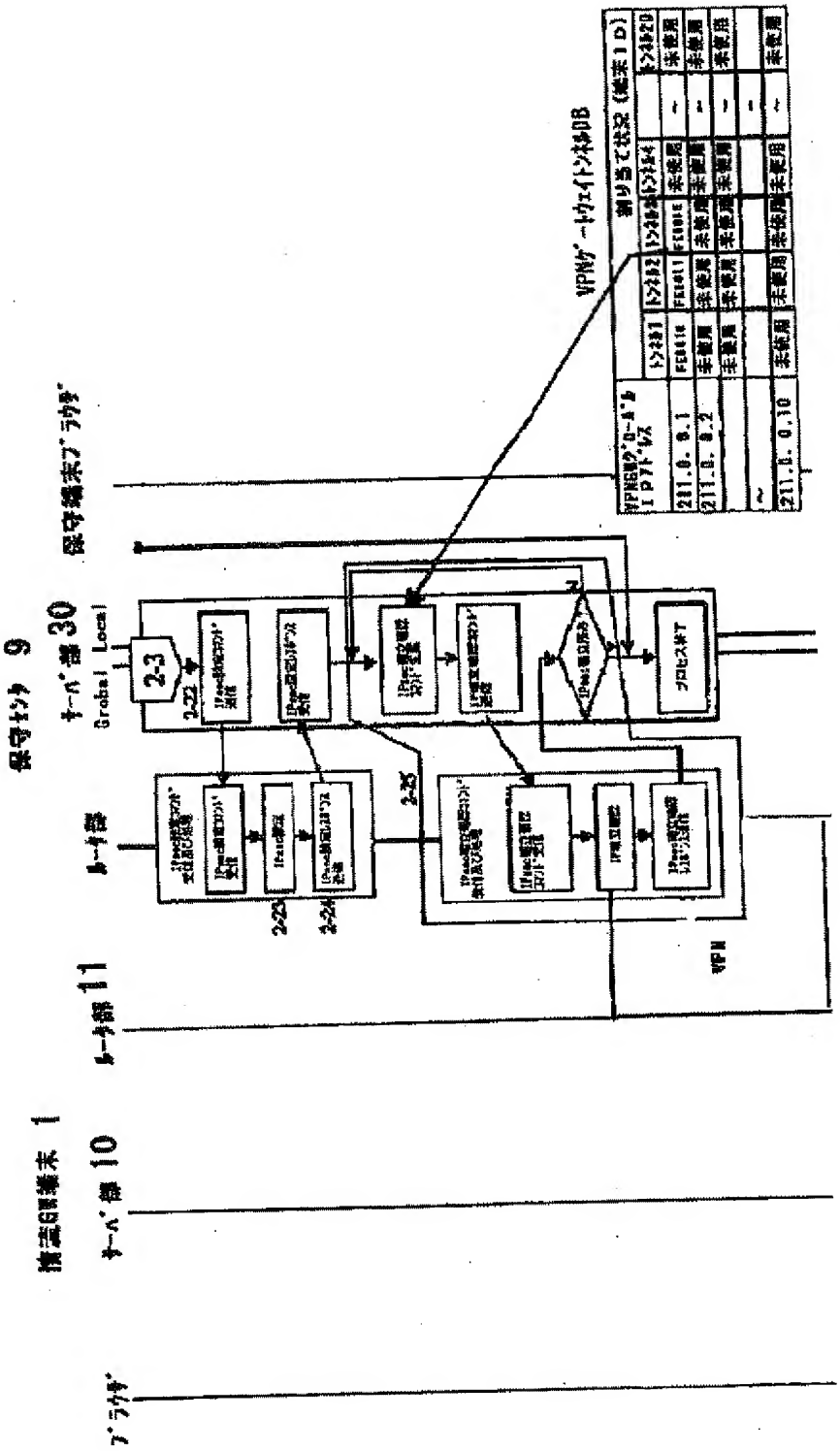
【図１６】



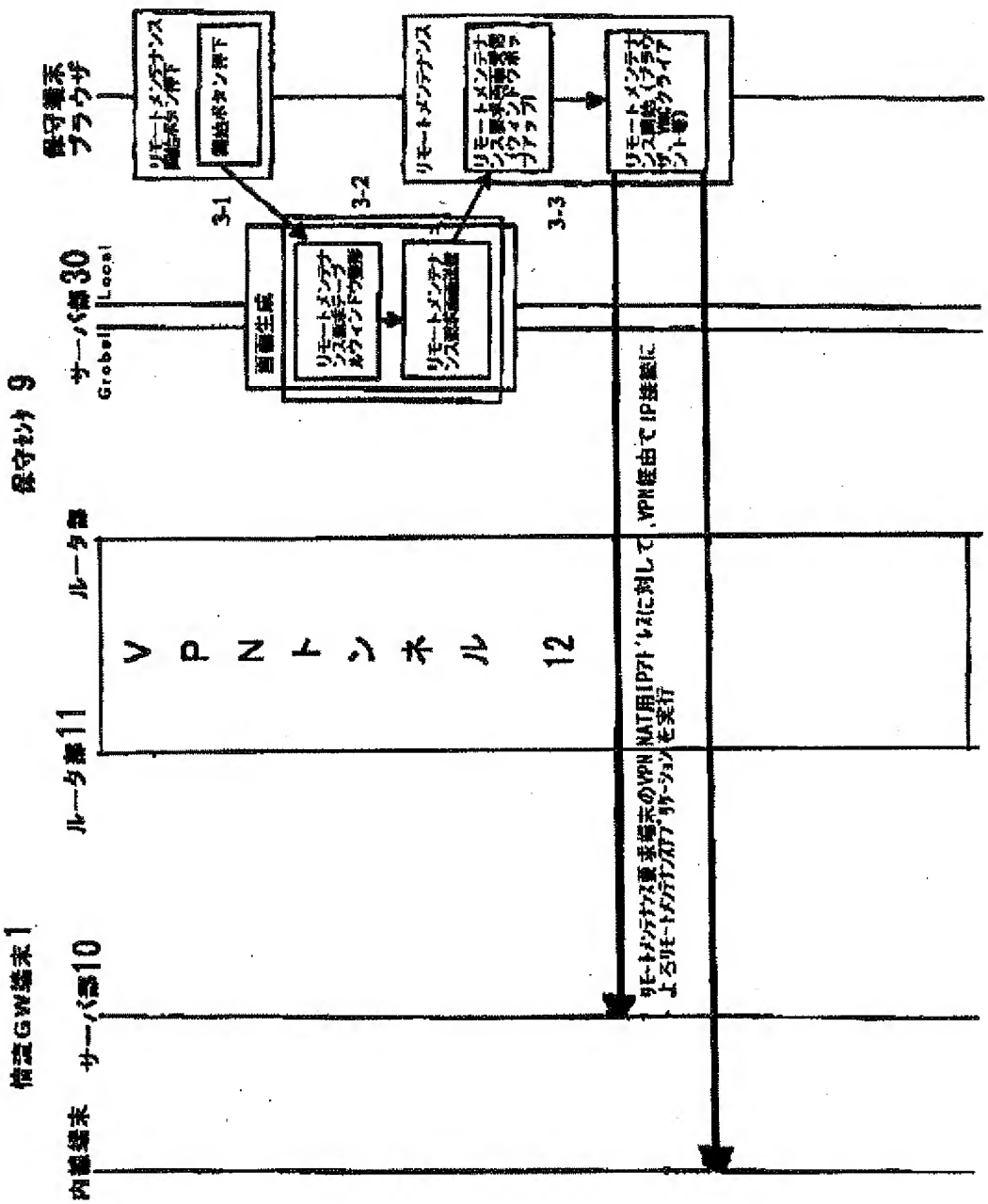
【図１７】


保守センタ
9
ルータ部
30
Group Local
2-2
保守端末グループ
VPNNATDB 91
リモートメンテナンス要求DB 92
VPNゲートウェイトンネルDB
VPNGWグループ
IPアドレス
211.0.0.1
211.0.0.2
211.0.0.3
211.0.0.10
未使用
情流店端末 1
ルータ部 10
ルータ部 11
ルータ部
2-3
出荷後情報
PreSharedKey
Secret-ID2
保守用VPNNAT用IPアドレス
ルータ用VPNNAT用IPアドレス
端末名=VPNNAT用グループ
受付番号
端末名VPNNAT用IPアドレス
VAIO

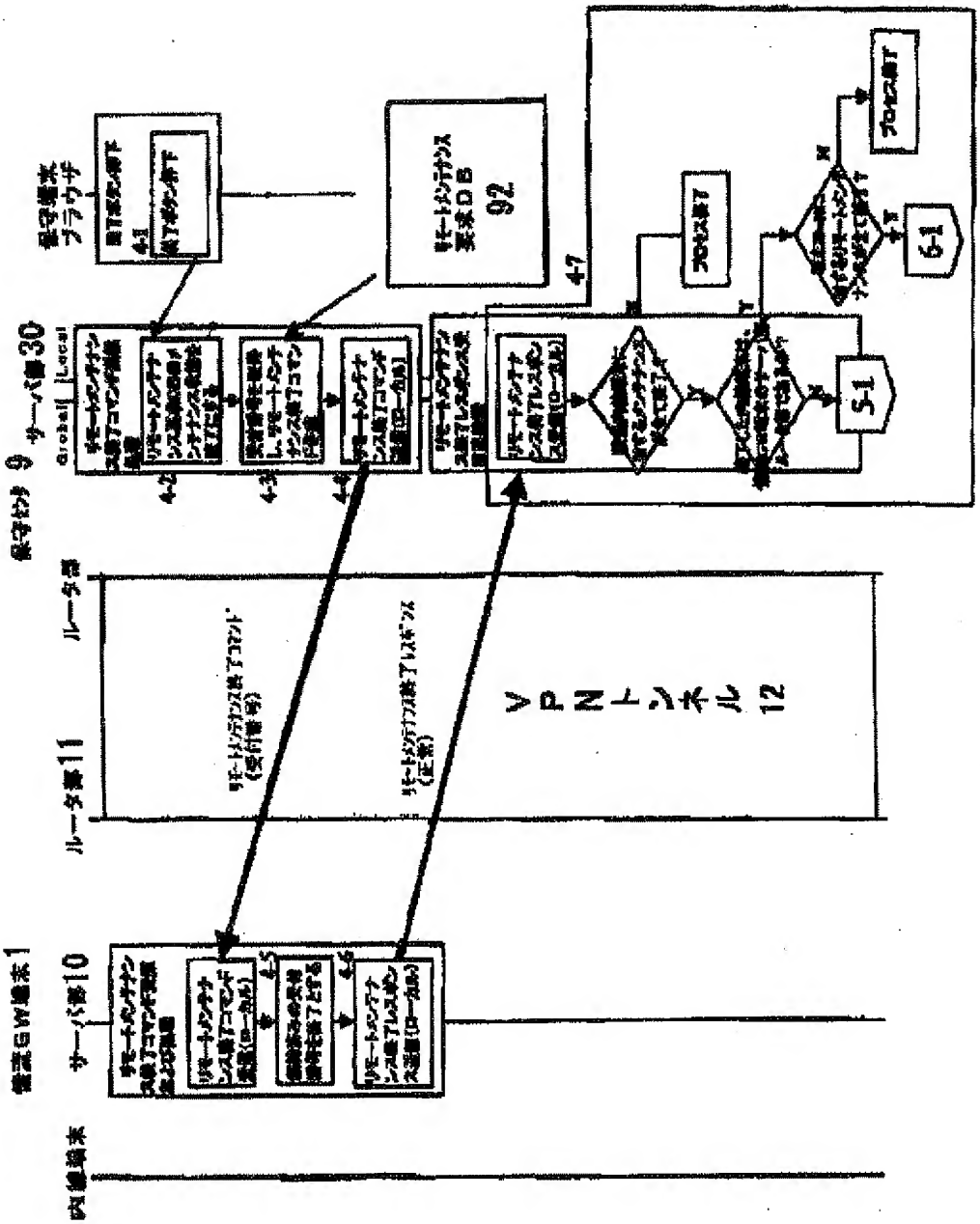
【図１８】


保守センタ 9
ルータ部 11
ルータ部 30
保守端末グループ
Global Local
2-3
2-22
2-23
2-24
2-25
VPNゲートウェイ装置DB
VPN
ルータ部
ルータ部 10
指定保守端末 1
グループ

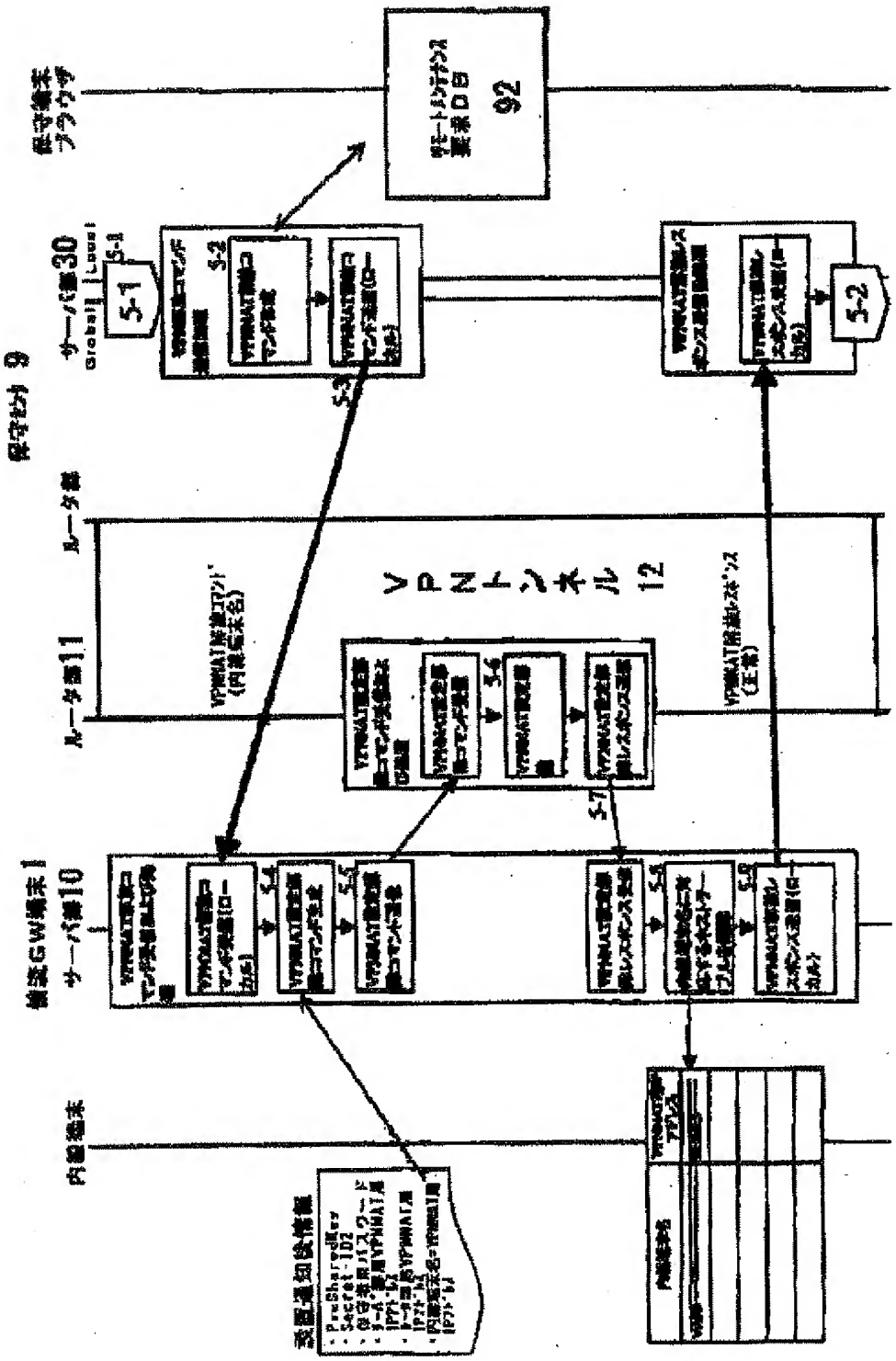
【図１９】


保守端末
ブラウザ
保守センタ 9
サーバ部30
Local
Global
ルータ部
ルータ部11
VPNトンネル 12
情報GW端末1
サーバ部10
内部端末
3-1
3-2
3-3
画面生成
VPNに対して、VPN経由でIP接続に

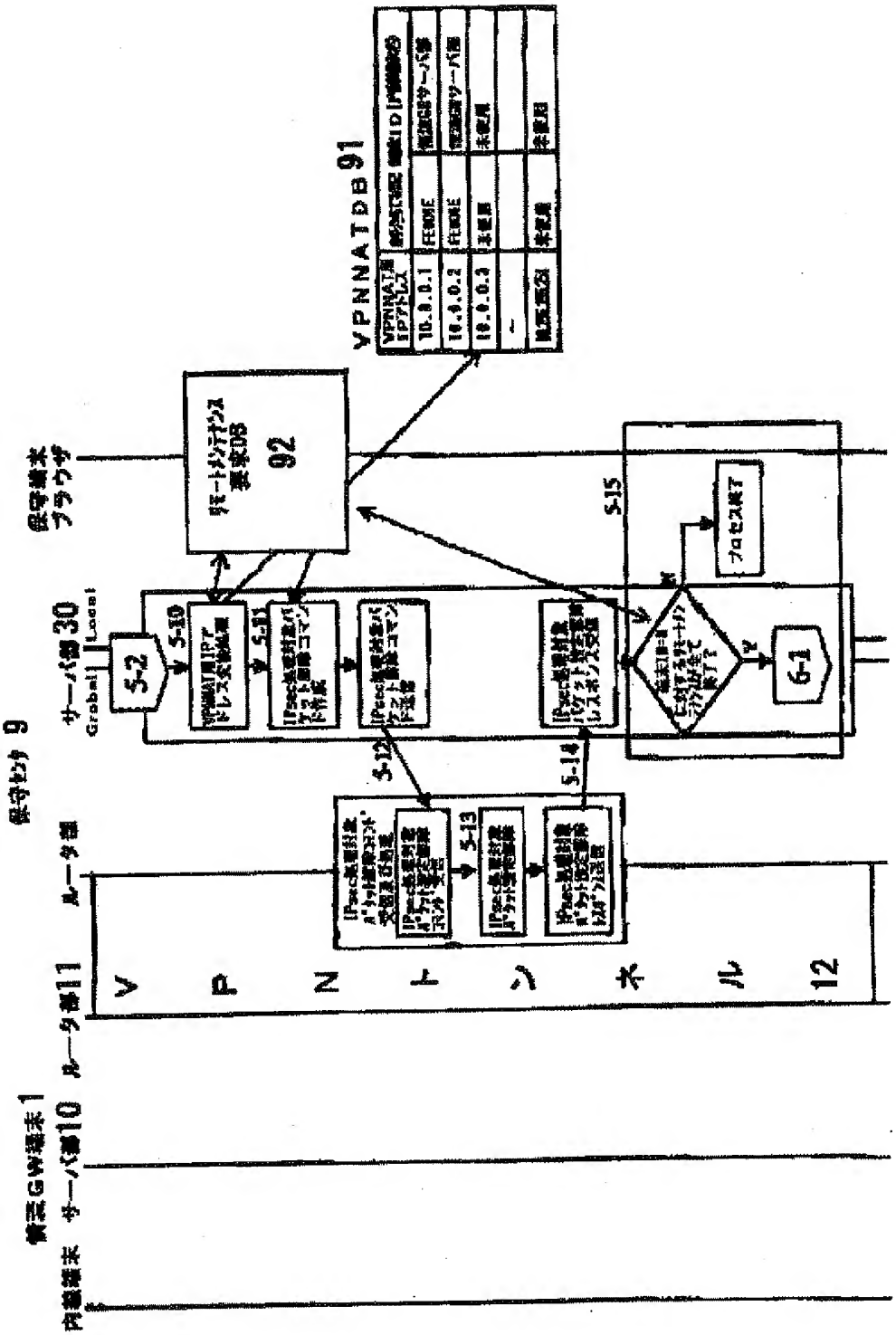
【図２０】



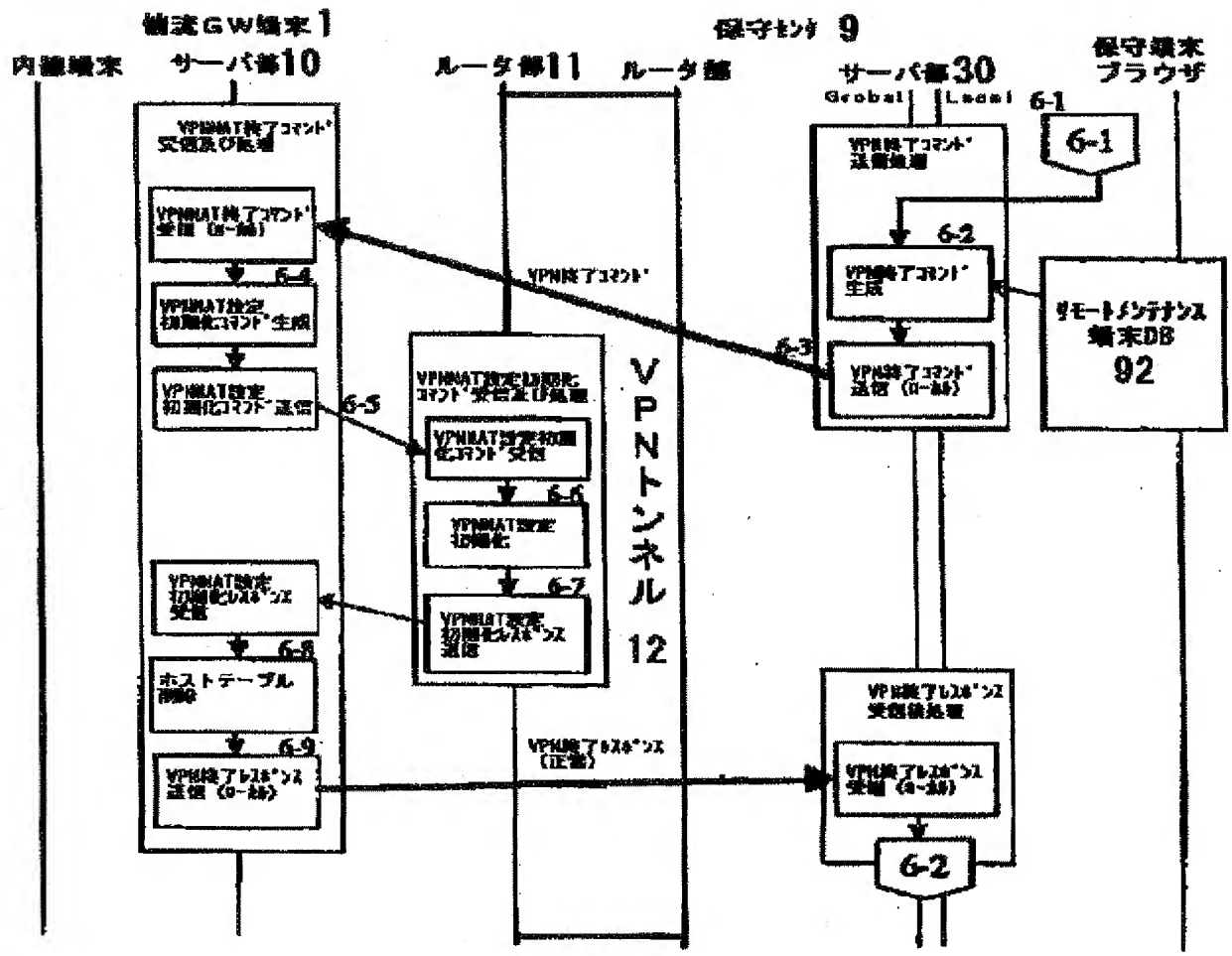
【図２１】


保守端末
ブラウザ
92
保守LAN 9
サーバ群30
5-1
5-2
5-3
ルータ群
ルータ群11
VPNトンネル 12
5-4
5-5
5-6
5-7
接続GW端末1
サーバ群10
内部端末
変更通知依頼書

【図２２】


VPNNATDB 91
VPNNAT用IPアドレス
10.0.0.1
10.4.0.2
10.0.0.3
FEMME
FEMME
未使用
未使用
保守端末
ブラウザ
メンテナンス
要求DB
92
サーバ部30
Global
Local
S-2
S-10
S-11
S-12
S-13
S-14
S-15
プロセス終了
6-1
保守セグ 9
ルータ部11
VPNトンネル
12
内部端末
構成GW端末1
サーバ部10
ルータ部

【図２３】



【図２８】

端末ＤＢ９０

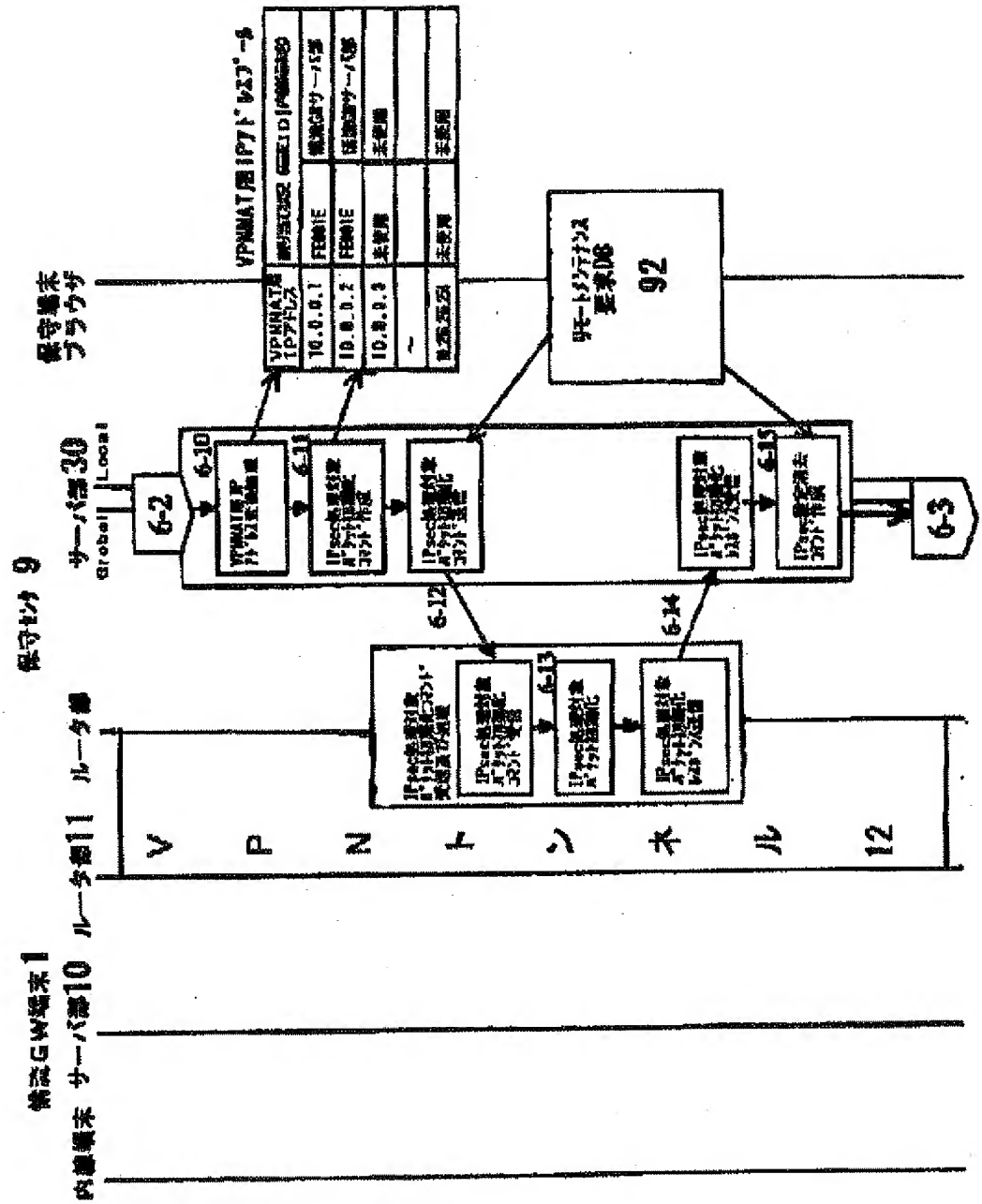
端末ID	PresharedKey	Secret-ID2	保守者用パスワード	サーバ部用 VPNNAT用 IPアドレス	ルータ部用 VPNNAT用 IPアドレス
FE001E	Hogehoge	Hkuitsu	01Pass	10.0.0.1	10.0.0.2

【図２９】

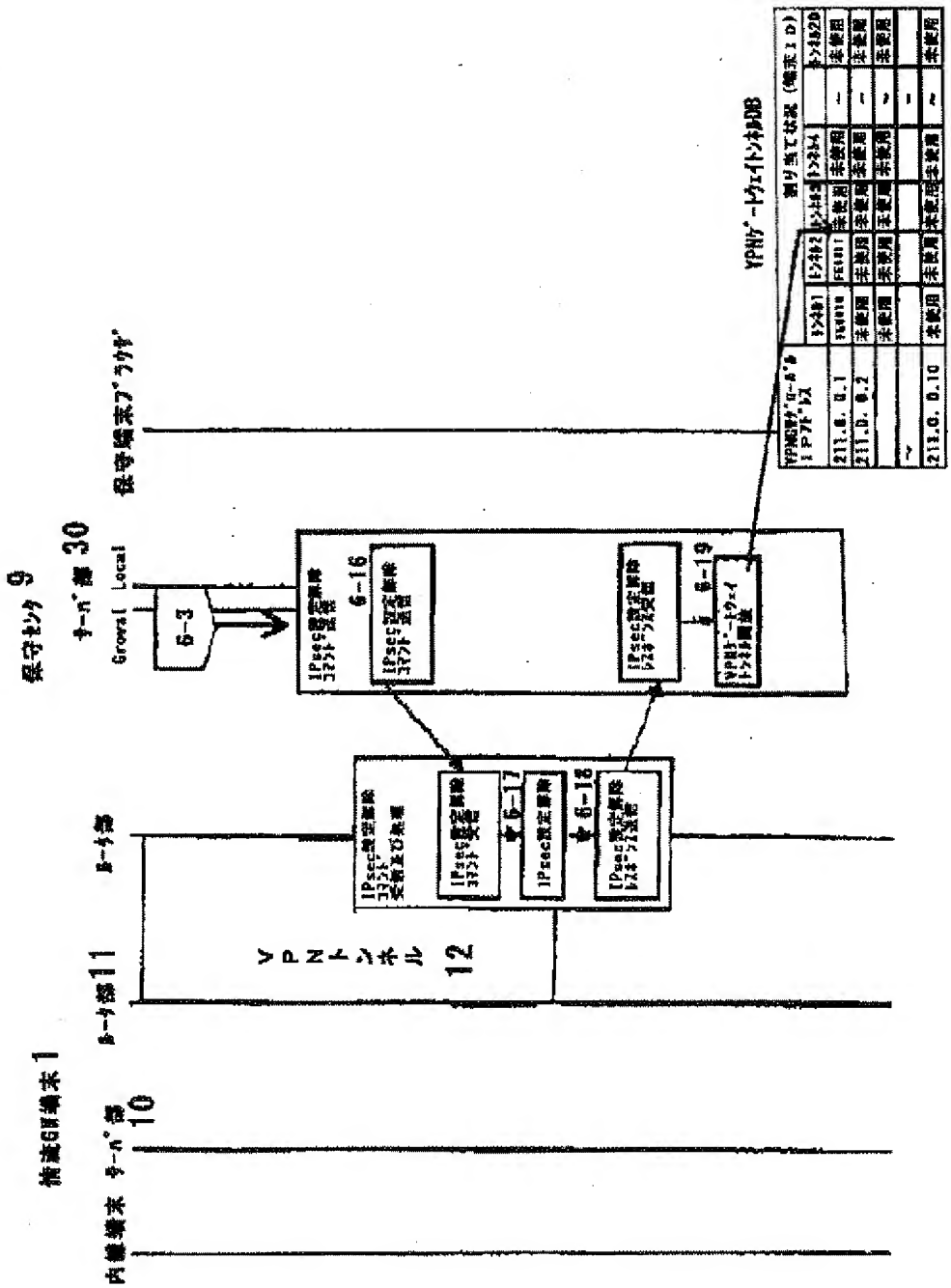
リモートメンテナンス要求ＤＢ９２

受付番号	端末ID	内線端末名	グローバルIPアドレス	要求者名	要求者レベル	電話番号	緊急度	要求内容	受信時刻	VPNNAT用IPアドレス	テーブル名	メンテナンス状態
1	FE001E	VAIO	211.0.4.3	山田	一般	0468xxx	緊急	…	17:23	10.0.0.03	VAIO	対応待ち

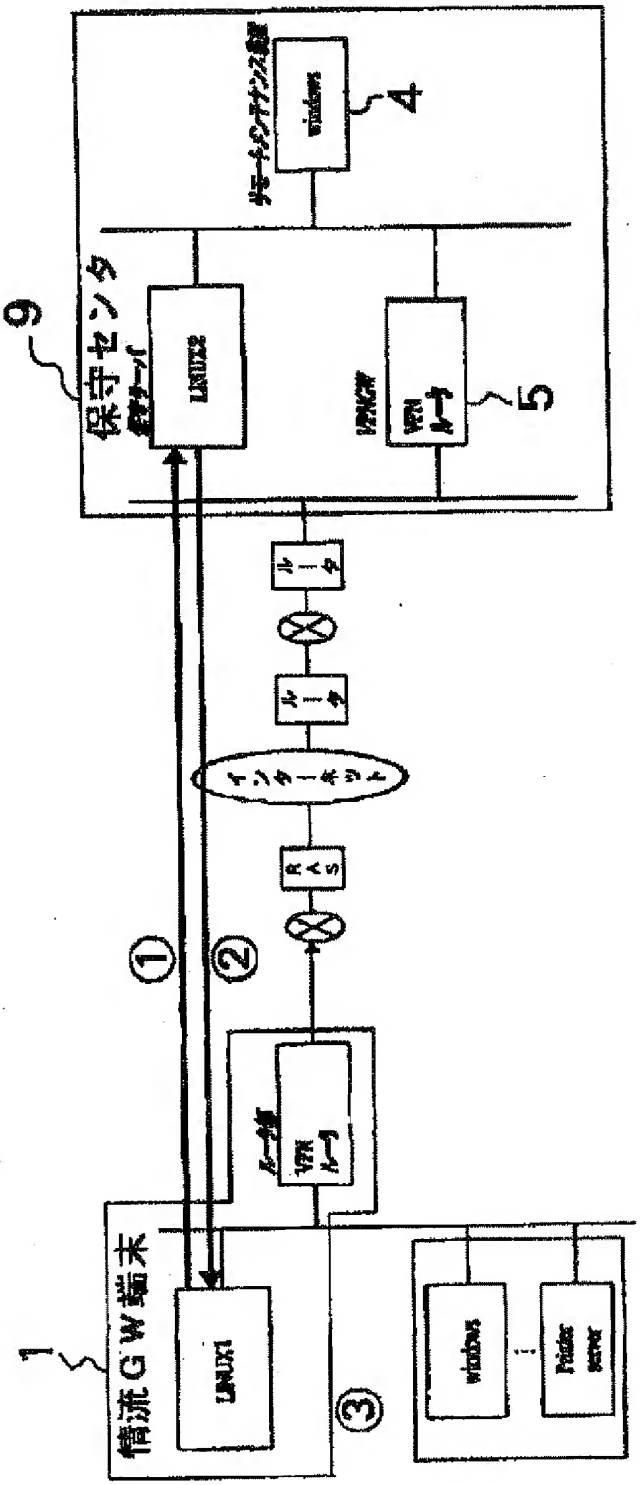
【図２４】


保守端末
ブラウザ
VPNNAT用IPアドレステーブル
VPNNAT用IPアドレス
10.0.0.1
10.0.0.2
10.0.0.3
FENNIE
FENNIE
未使用
未使用
未使用
保守センタ 9
サーバ部30
Global
Local
6-2
6-10
6-11
6-12
6-13
6-14
6-15
6-3
特定メンテナンス装置06
92
構成GW端末1
内線端末
サーバ部10
ルータ部11
ルータ部
VPNトンネル12

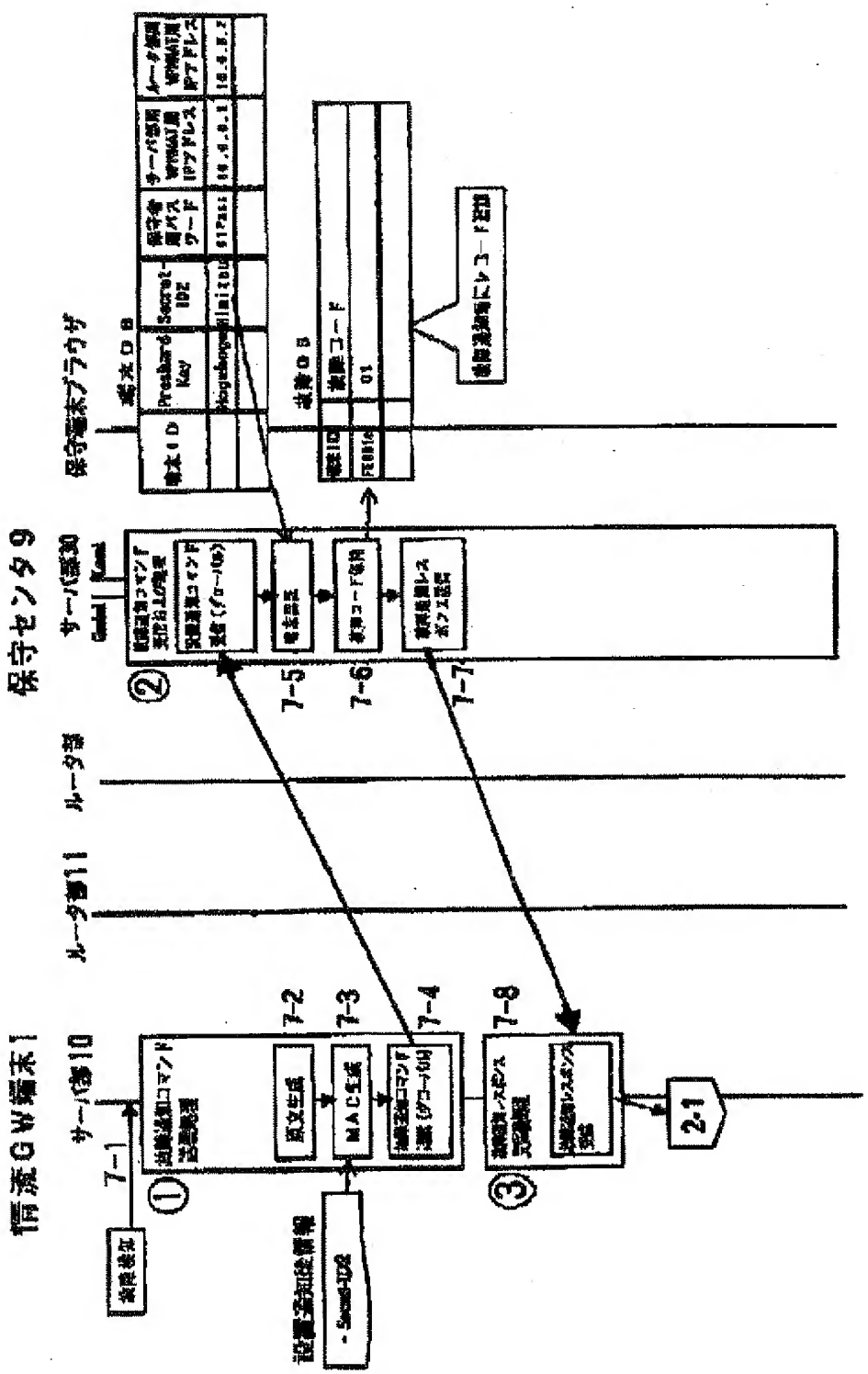
【図２５】


保守センタ 9
ネットワーク部 30
保守端末ブラウザ
Global Local
6-3
6-16
6-19
VPNゲートウェイトンネル制御DB
VPNゲートウェイ
IPアドレス
割り当て状況（端末ID）
211.0. 0.1
211.0. 0.2
211.0. 0.10
未使用
使用
拠点6IP端末
内線端末
ネットワーク部 10
ルータ部 11
VPNトンネル 12
ルータ部
6-17
6-18

【図２６】


windows
4
保守センタ
9
LINUX
VPN
5
ルータ
ルータ
インターネット
RAS
①
②
③
情流ＧＷ端末
1
LINUX
VPN
windows
Folder server

【図２７】


保守センタ９
情流ＧＷ端末１
サーバ部１０
ルータ部１１
ルータ部
サーバ部３０
保守端末ブラウザ
7-1
7-2
7-3
7-4
7-5
7-6
7-7
7-8
2-1

【図３０】

VPNNATDB91

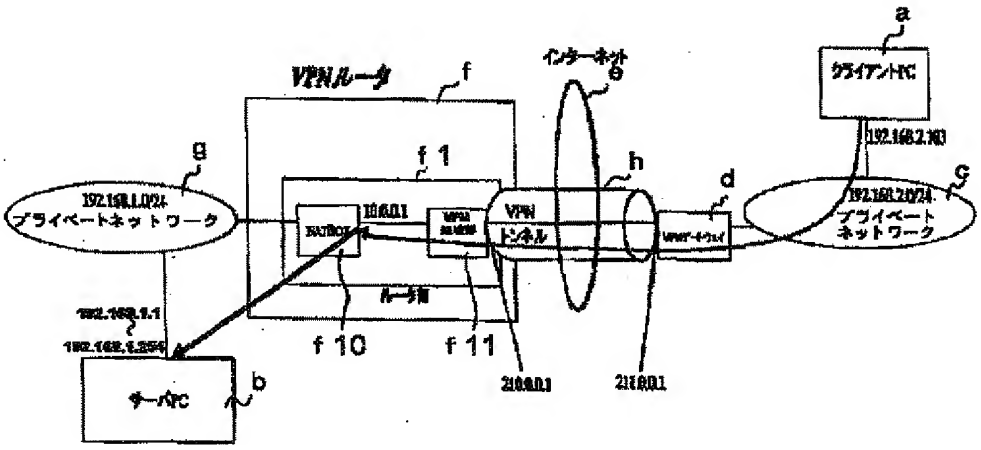
VPNNAT用IPアドレス	割り当て状況（端末ID	内線端末名）
10.0.0.1	FE001E	情流GWサーバ部
10.0.0.2	FE001E	情流GWサーバ部
10.0.0.3	FE001E	VAIO
～		
10.255.255.254	未使用	未使用

【図３１】

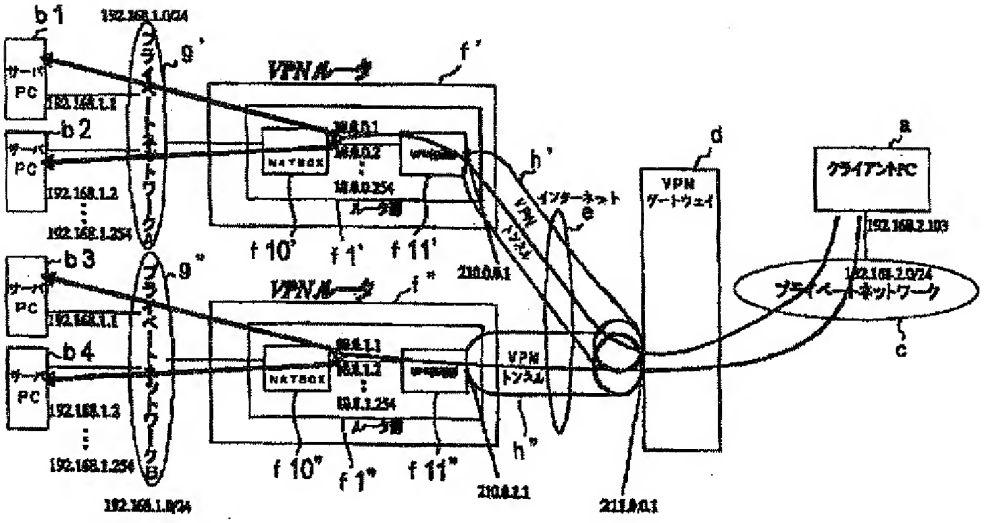
リモートメンテナンス要求DB　９２

受付番号	端末ID	内線端末名	グローバルIPアドレス	要求者名	要求者レベル	電話番号	緊急度	要求内容	受信時刻	VPNNAT用IPアドレス	テーブル名	メンテナンス状態
1	FE001E	VAIO	211.0.4.3	山田	一般	0468xxx	緊急	…	17:23	10.0.0.3	VAIO	終了

【図３２】



【図３３】


b1
b2
b3
b4
g'
g"
VPNルータ
f'
f"
NATBOX
f10'
f1'
f11'
f10"
f1"
f11"
h'
h"
インターネット
e
VPN
ゲートウェイ
d
クライアントPC
a
プライベートネットワーク
c